工控系统网络安全等级测评评估研究

朱晓鹏[1,2],黄文财[1,2],钟远生[1,2],吴　耿[1,2]
(1. 广东产品质量监督检验研究院,广东 广州 510670;
2. 国家市场监管重点实验室(智能机器人安全),广东 广州 510670)

摘　要:针对当前工控系统网络安全等级测评计算繁琐、权重计算简单、缺乏工控系统的针对性和评估结果具有随机性和模糊性的问题,研究一种工控系统网络安全等级测评评估方法。绘制以网络安全等级测评为基础的工控系统典型框架,分析工控系统相对安全通用类等级测评在评估指标上的差异,并采用主观赋权法确保上述评估指标差异在工控系统权重赋值中倾斜的合理性,应用客观赋权法保证权重赋值的科学性,使用组合赋权法综合考量主客观赋权优点,确保工控系统评估指标权重赋值的合理性和科学性;使用专家云模型结合组合赋权法获取的组合权重,得出工控系统网络安全等级测评评估结果,再基于云模型的概率统计和模糊数学,克服繁琐的计算和评估结果的模糊性和随机性;最后,将该方法应用于某大型化工产业工控系统,结果表明该系统等级测评结果为良,与预案评审结果一致,验证了该方法在网络安全等级测评中的有效性和适用性。

关键词:工控系统;网络安全;等级测评;组合赋权;专家云模型
中图分类号:TP393.038　　**文献标识码**:A　　**文章编号**:1673-629X(2023)12-0149-07
doi:10.3969/j.issn.1673-629X.2023.12.021

Research on Evaluation of Network Security Level of Industrial Control System

ZHU Xiao-peng[1,2], HUANG Wen-cai[1,2], ZHONG Yuan-sheng[1,2], WU Geng[1,2]
(1. Guangdong Testing Institute of Product Quality Supervision, Guangzhou 510670, China;
2. National Key Laboratory for Market Supervision (Intelligent Robot Safety), Guangzhou 510670, China)

Abstract: Aiming at the problems of complex calculation, simple weight calculation, lack of pertinence of industrial control systems, and randomness and fuzziness of evaluation results in the current industrial control system network security level evaluation, a method for evaluating the network security level of industrial control systems is studied. A typical industrial control system framework based on network security level assessment is drawn, the differences in evaluation indicators between industrial control systems and general security level assessments is analyzed, and subjective weighting methods are used to ensure the rationality of the above evaluation indicator differences in the weighting of industrial control systems. The objective weighting methods are used to ensure the scientificity of weighting, and combined weighting methods are used to comprehensively consider the advantages of subjective and objective weighting, which ensures the rationality and scientificity of the weight assignment of industrial control system evaluation indicators; using the combination weights obtained by combining the expert cloud model with the combination weighting method, the evaluation results of the network security level of the industrial control system are obtained. Based on the probability statistics and fuzzy mathematics of the cloud model, the fuzziness and randomness of the tedious calculation and evaluation results are overcome. Finally, the proposed method is applied to a large chemical industry industrial control system, and it is showed that the system level evaluation is effective, consistent with the plan evaluation results, The effectiveness and applicability of the proposed method in network security level evaluation are verified.
Key words: industrial control system; network security; grade evaluation; combination empowerment; expert cloud model

0　引　言

工控系统是一种集监控与数据采集、分布式控制、可编程逻辑控制、人机交互等组件为一体,保证工业领域和关键基础设施执行自动化、过程控制与监控的管

收稿日期:2023-01-13　　**修回日期**:2023-05-16
基金项目:国家市场监督管理总局科技计划项目(2022MK095)
作者简介:朱晓鹏(1982-),女,工程师,研究方向为网络安全、等级保护测评;通信作者:黄文财(1995-),男,工程师,硕士研究生,研究方向为等级保护测评、软件测评。

控系统[1],成熟应用于能源、交通、水利、化工、核设施、国防科技工业等关键基础设施,一旦发生设备损毁、功能丧失或者关键数据泄露,严重程度可危及社会公共利益,甚至是国家安全,因此保障工控系统网络安全已经上升为国家层面的安全战略[2]。

针对工控系统的网络安全,ISA(国际自动化协会)99 制定了标准《工业过程测量、控制和自动化网络与系统信息安全》[3];美国为了保护其关键基础设施的工控系统,制定了《工业控制系统(ICS)安全指南》[4];欧洲针对工控系统的完整性、可用性和保密性,提出了 ITSEC 信息技术安全评价准则[5-7];中国为了加强工控系统信息安全防护措施,制定了《工业控制系统信息安全防护指南》[8];为了确保工控系统网络安全的落实适应国家环境、企业文化、人员管理体系,国家市场监督管理总局颁布 GB/T 22239-2019《信息安全技术—网络安全等级保护基本要求》(等保 2.0)[9],该标准将工控系统划分为新型应用安全扩展项,并形成一个安全管理中心,结合安全计算环境、安全区域边界、安全通信网络的“一个中心,三重防护”的工控系统网络安全总体体系架构[10]。通过安全设备和安全技术手段加强网络安全防护措施,集中管控系统、安全和审计工作,让工控系统从被动、静态、单点、粗放型防护向主动、动态、整体、精准型安全防护转变[11]。等级保护工作阶段包括定级、备案、安全建设整改、等级测评和监督检查。等级测评应用到工控系统具有以下优点:(1)判断工控系统的物理环境、安全区域、安全通信、系统管理和制度、体系、人员管理等安全措施的有效性,综合评判工控系统是否具备国家要求的安全防护能力;(2)分析等级测评结果中异常数据,定位安全防护措施的漏洞和缺陷,为改善工控系统网络安全提供依据;(3)等级测评的过程是动态的,根据多次测评与整改,不断验证工控系统的安全保护能力,实现工控系统安全防护能力的持续调优[12]。因此,等级测评有助于解决国内工控系统面临的威胁和存在的主要问题。然而现有的体系没有直接设定等级测评结论的判定方法,因此,等级测评已成为众多学者迫切研究的方向。目前等级测评有定量法、定性法和两者相结合的方法、模糊综合评价法、加权评估法等[13],然而现有的评估方法具有以下缺陷:

(1)计算繁琐;统计类型众多,包括大类、控制点、具体检查项;映射关系复杂,具体检查项需映射到具体的测评对象,映射关系包括一对一、一对多、多对多,双方关系显网络状,交错复杂,易造成测评过程逻辑混乱。

(2)权重计算简单;权重计算只是根据具体检查项重要程度按主观经验直接赋权,缺乏科学性[14]。

(3)缺乏工控系统的针对性,统计分数和计算权重只是在安全通用类上直接叠加,没有考虑工控系统在安全区域边界、安全物理环境和安全建设管理等类型上计算分数和赋值权重的差异。

(4)评估过程、结果的模糊性和不确定性,根据具体检查项与预期测评的一致性,划分为符合、部分符合、不符合、不适用四种评定,缺乏实际的定量数据[15],且测量方法包含大量访谈的主观评估,也需生成综合评估模糊结果。

该文设计一种工控系统网络安全等级测评方法,可综合评估工控系统的等级测评结果。首先,绘制基于网络安全等级测评的典型工控系统框架,分析其差异性;其次,使用主观赋权法确保工控系统评估指标权重倾斜的合理性,应用客观赋权法保证权重的科学性,采用组合赋权法综合考量工控系统评估指标权重赋值的合理性和科学性;最后,基于专家云模型,减少繁琐的计算,克服综合评价的模糊性与随机性问题。

1 网络安全等级测评中工控系统差异性分析

分析基于网络安全等级测评的工控系统典型框架,解析工控系统相对安全通用类等级测评的差异性,为网络安全等级测评适用于工控系统提供理论基础。

通过逐一分析、拆解工控系统,结合网络安全等级保护的建设体系,根据“一个中心,三重防护”的纵深防御思想[16],绘制了基于网络安全等级保护的工控系统典型框架(见图 1),其特征为:

(1)安全区域边界划分;根据业务和安全需求,工控系统可划分为生产管理中心、网络交换中心、信息管理中心和安全管理中心等,它们之间的通信由安全防护设备隔离,形成不同系统的安全区域边界,保证不同区域网络互联互通的同时,也实现边界保护、访问控制、入侵防范的内部安全防御。

(2)计算环境的安全防护;安全区域边界内部设备可通过网络交换中心连接起来,基于身份鉴别、安全审计、入侵防范、可信验证等安全方法,保证服务器、网络、终端、安全等设备和数据、应用软件、应用系统等对象的安全防护,在生产管理中心,依据对应的工控安全协议确保不同层级的生产安全,从而保证安全的计算机环境。

(3)通信网络的安全防护;工控系统基于防火墙、隔离装置形成了内外分离的网络架构,公共数据区访问工控系统内部需经过认证访问,在通信传输过程具有加密防护系统和校验机制,确保数据的保密性、完整性、可用性等。

(4)集中安全管理;工控系统具有独立管理区域

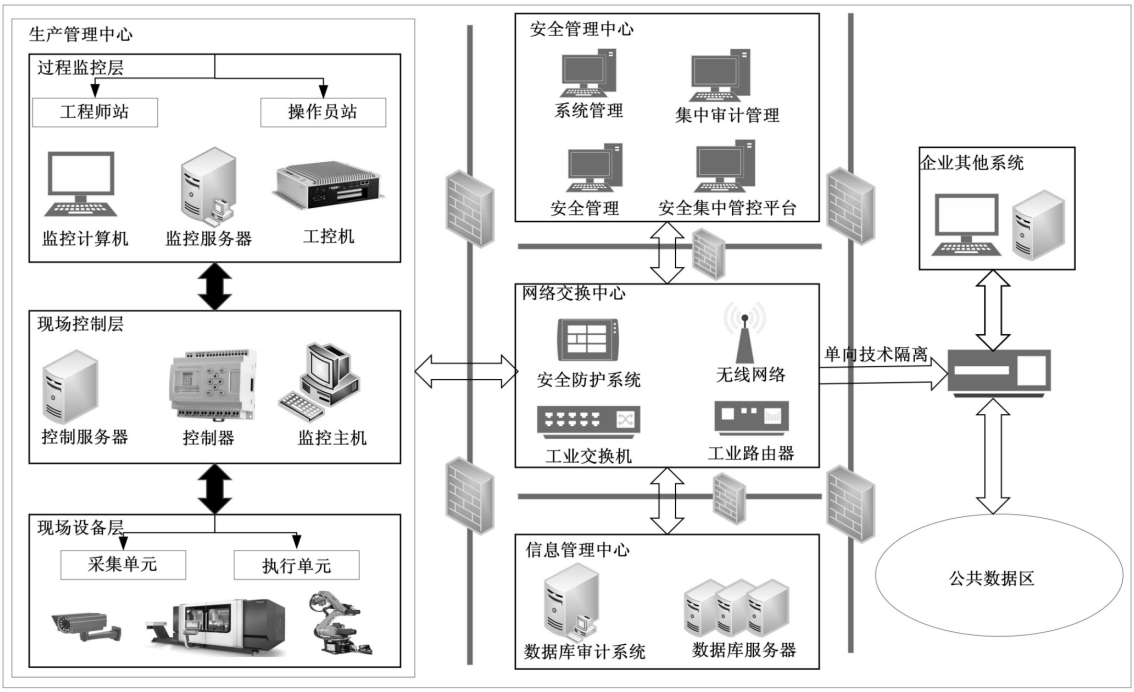


图 1　基于网络安全等级测评的工控系统典型框架

的安全管理中心,是按照安全策略集中管控安全管理、集中审计、系统管理等相应设备,统一监控、分析、管理安全事件,构成了安全管理的“大脑”,提高工控系统安全运维管理的有效性。

网络安全等级测评中,工控系统相对安全通用类的差异性:

(1)物理环境的差异;工控系统所处物理环境一般较差,对物理防护要求也会更高,特别是工控系统部分设备属于室外控制设备,需加强各类安全措施完成物理防护。

(2)通信网络的差异;工控系统在网络框架上具有分层分域特点,生产管理中心划分为现场设备层、现场控制层、过程监控层;工控系统与企业其他系统划分为两个区域,由于企业其他系统与公共数据区的互联网相连,采用单向隔离技术,保证数据流只单向流向企业其他系统。

(3)区域边界的差异;工控系统禁止 WEB,FTP,E-Mail等通用网络服务穿越安全区域边界,且工控系统设备复杂且众多,着重于实时性[17],因此青睐于无线通信,增加了无线通信的加密、授权、识别等要求。

(4)计算环境的差异;工控系统强调可用性,因此对控制设备的安全有更高的要求,包括访问授权、外设接口专设专用,上线前的检查和及时更新固件。

(5)安全建设管理的差异;工控系统重要设备专设专用,每一设备都有其特定用途,相对通用设备具有一定特殊性,需专业机构安全检测保证设备的安全性[18];且外包软件需签署约束条款,防止关键技术的泄露和扩散。

2　工控系统权重计算

针对主观经验直接赋权,权重计算简单,运用层次分析法、CRITIC 客观赋权法分别计算主观权重和客观权重,采用组合赋权法综合考量主客观权重优点,提高权重的合理性、科学性。

2.1　等级测评评估指标

为了保证指标的权威性,选取 GB/T22239-2019 的评估指标作为工控系统等级测评评估指标,如图 2 所示。

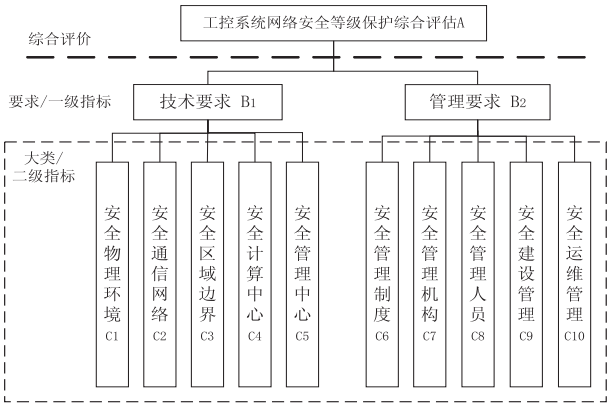


图 2　工控系统网络安全等级测评指标

2.2　主观权重计算

考虑工控系统与安全通用类在等级测评上的差异,在安全区域边界、安全计算环境、安全物理环境、安全通信网络和安全建设管理上权重值会有所倾斜,采用专家专业知识和经验的主观赋权法,保证工控系统的等级测评权重的合理性是有必要的。该文运用层次分析法构建二级指标、一级指标、综合评价的层次结

构,专家根据等级测评中各项指标对安全业务的重要程度,构建判断矩阵,检验一致性后获取主观权重(SW,如公式(1)所示),组合二级指标层中的权重,计算对应一级指标层中的权重值,并获取综合评价的权重值,提高权重的合理性。

$$SW_i = \frac{\left(\prod_{j=1}^{n} a_{ij}\right)^{\frac{1}{n}}}{\sum_{k=1}^{n}\left(\prod_{j=1}^{n} a_{ij}\right)^{\frac{1}{n}}}, \quad i = 1,2,\cdots,n \tag{1}$$

2.3 客观权重计算

为了克服权重计算主观性过强的问题,基于实际测量数据构建客观权重,增加权重的科学性。文中数据来源于文献[19],由于等级保护先是安全建设整改,再执行等级测评,测评结果不符合占比较低,甚至出现多份不同数据、同一指标都是符合的极端数据,导致基于数字越大则指标越重要的熵权法和标准离差法等客观赋权并不适用。该文选择既考虑数据取值差距的大小,同时兼顾数据之间的相关性的 CRITIC 客观赋权法,采用标准差计算数据差距的大小,差距越大,则权重越高;采用皮尔逊相关系数统计数据间的相关性,若双方数据具有较弱的正相关,其冲突性较大,则权重较高,其计算的客观权重如公式(2)所示。

$$KW_j = \frac{\eta_j \varepsilon_j}{\sum_{j=1}^{n}(\eta_j \varepsilon_j)} = \frac{\eta_j \sum_{k=1}^{n}(1 - r_{kj})}{\sum_{j=1}^{n}\left(\eta_j \sum_{k=1}^{n}(1 - r_{kj})\right)} \tag{2}$$

其中,ε_j 表示皮尔逊相关系数,r_{kj} 是数据 k 和 j 之间的相关系数,η_j 表示标准差,x_{ij},$\bar{x}$ 分别表示数据 i 第 j 个数值和第 j 个数据的平均值。

2.4 组合权重计算

为了确保主观赋权的随机性控制在一定范围内,又能考虑指标数据之间的内在统计规律,采用组合赋权法综合考量主客观权重优点,弥补单一赋权带来的不足,提高权重的合理性、科学性,计算如公式(3)所示,得到的主客观及组合权重如表 1 所示。

表 1 指标的主客观及组合权重值

一级指标	组合权重 W	二级指标	主观权重 SW	客观权重 KW	组合权重 W
B1	0.585	C1	0.048	0.078	0.062
		C2	0.096	0.056	0.075
		C3	0.073	0.091	0.083
		C4	0.145	0.172	0.161
		C5	0.238	0.168	0.204
B2	0.415	C6	0.046	0.101	0.070
		C7	0.099	0.073	0.087
		C8	0.049	0.084	0.065
		C9	0.099	0.064	0.081
		C10	0.107	0.113	0.112

$$ZW_j = \frac{\sqrt{SW_j KW_j}}{\sum_{j=1}^{n}\sqrt{SW_j KW_j}} \tag{3}$$

2.5 权重的修正

等级测评中涉及该 10 个安全指标,在工控系统实际测评中,也可能只涉及其中几类[15],因此需要修正权重值。设 $WQ_i(i = 1,2,\cdots,n)$ 是不涉及测试的一个或多个安全指标的权重,则权重的修正如下:

$$W_j = \frac{ZW_j}{\sum_{j=1}^{10} ZW_j - \sum_{i=1}^{n} WQ_i} \tag{4}$$

3 网络安全等级测评评估

采用基于专家经验的云模型生成以自然语言描述等级测评综合评估结果,克服测评层级众多、映射关系复杂导致的计算繁琐和评估的模糊性与不确定性的问题。云模型是一种以概率统计和模糊数学为基础,采用数字特征表示隶属云,达到定性概念与定量值相互转换的数学模型[20],相较于用精确数字去解决模糊问题的传统隶属函数,其隶属度细微变化,并不影响到云的整体特征,充分考虑了评估过程和评估结果的随机性、模糊性以及两者之间的关联性的问题,更加彻底展示模糊性[21]。鉴于此,该文采用云模型理论评估网络安全等级测评结论的等级,其步骤如下:

(1)标准云的绘制;根据文献[15]的等级划分,设置等级测评结论 R = {R1,R2,R3,R4} 和对应的评分区间,如表 2 所示,划分为优、良、中、差,参考文献[11]和文献[16]设置对应评分区间的约束条件,利用其评分区间的有效论域[$M_{\min}$,$M_{\max}$],采用指标近似法(公式(5))求出等级区间的云模型特征值(如表 2 所示),再将其绘制成标准云模型,作为隶属度的衡量标准。

$$\begin{cases} Ex = (M_{\min} + M_{\max})/2 \\ En = (M_{\max} - M_{\min})/6 \\ He = kEn \end{cases} \tag{5}$$

其中,k 为熵和超熵之间的关系数值,一般取 0.1。

(2)具体检查项的划分;针对控制类具有部分符合的模糊性的问题,将统计结果深入到具体检查项,根据检查项中检查对象和条目的重要程度,将其划分为一般、重要、关键三个层级。

(3)统计大类、控制类;统计大类、控制类的符合、部分符合、不符合、不适用的符合情况。

(4)选择大类作为评价指标(图 2 中指标);若该指标下面的所有具体检查项都符合则直接赋于满分特征参数(100,0,0),若该指标所具备的具体检查项都不符合,则给出最低分特征参数(0,0,0),若该指标部分满足具体检查项,则采用专家经验云模型评分。

(5)基于专家经验的评分;根据测评具体项总结情况,专家基于自身的经验和知识,根据测评具体项符合指标要求的符合程度,符合度越高则分值也越高的原则给出最高分,考虑到指标的模糊性,再给出最低分,构建模糊区间,参考区间如表 2 所示,取值范围为[0,100]。

表 2　等级测评结论

编号	等级测评结论	评分区间 $[M_{\min},M_{\max}]$	云模型特征参数(Ex,En,He)	约束条件
R1	优	[90,100]	(95,1.667,0.166 7)	被测工控系统不会出现中、高等级安全风险
R2	良	[80,90)	(85,1.667,0.166 7)	被测工控系统不会出现高等级安全风险
R3	中	[70,80)	(75,1.667,0.166 7)	被测工控系统不会出现高等级安全风险
R4	差	[0,70)	(35,11.667,1.166 7)	被测工控系统存在严重安全漏洞,可能出现高等级安全风险

(6)专家云模型计算;专家给出了具有模糊区间的最高分和最低分,采用指标近似法(公式(5))求出该专家云模型特征值。

(7)评价指标云模型计算;设第 $j(j=1,2,\cdots,n)$ 个专家根据自身的专业知识给出第 $i(i=1,2,\cdots,m)$ 指标的云模型特征参数为 $\text{experts}_j(\text{Ex}_i,\text{En}_i,\text{He}_i)$,指标 i 上的各专家云模型特征参数组合为 $\text{experts}(\text{Ex}_i,\text{En}_i,\text{He}_i)$,则专家组合第 i 个指标的云模型(S_i)为:

$$S_i=\begin{cases}(100,0,0) & \text{全部符合}\\ f(\text{experts}(\text{Ex}_i,\text{En}_i,\text{He}_i),\text{ew}) & \text{部分符合}\\ (0,0,0) & \text{都不符合}\end{cases} \tag{6}$$

其中,$\text{ew}=[\text{ew}_1,\text{ew}_2,\cdots,\text{ew}_i]$ 是专家权重的集合,取值为平均值 $\text{ew}_i=1/\sum_{i=0}^{n} i$。$f(x,y)$ 为组合 n 位专家的云模型,第一个参数是云模型组合,第二个参数为对应权重组合,通过加权组合计算得到指标结果为(Ex,En,He),其计算方法如公式(7)所示。

$$\begin{cases}\text{Ex}=\sum_{i=1}^{m}\text{Ex}_i W_i\\ \text{En}=\sqrt{\sum_{i=1}^{n}\text{En}_i^2 W_i}\\ \text{He}=\sum_{i=1}^{n}\text{He}_i W_i\end{cases} \tag{7}$$

(8)工控系统等级测评综合评估结果生成;将指标结合组合权重的赋权值通过公式(7)依次加权组合成一级指标、综合评价的云模型的特征参数,绘制成云模型,生成综合云模型的基本形态,与标准模型比较,进而判断一级指标和综合评价云模型的隶属度,再结合表 2 的评估等级,生成工工控系统等级测评综合评估结果。

4　等级测评评估方法验证

选取某大型化工工控系统为例,该化工行业设施作为国内关键基础设施,若网络安全受到威胁,可能危及社会公共利益和国计民生,甚至是国家安全,因此,对该化工工控系统做网络安全等级保护,完成等级测评,综合评判该化工工控系统是否具备国家要求的安全保护能力是很有必要的。根据该化工工控系统的实际情况,选取等级保护第三级进行等级测评。记录具体检查项符合程度,统计大类、控制类符合情况,利用上述方法测评其网络安全是否符合要求,由前述直接参与等级测评具体检查项测评的 6 位专家,根据测评总结资料,按照符合指标要求的程度给出最高分和最低分,构建模糊区间,打分时既考虑了工控系统的实际情况又综合考虑了丰富的从业经验和专业知识,因此评分结果相对科学、可靠。采用指标近似法(公式(5))求出该专家云模型特征值,结果如表 3 所示,通过组合专家云模型(公式(6))计算评价指标云模型。二级指标的云模型特征参数通过公式(7)结合组合赋权法的权重(如表 4 所示),获取等级综合评价,其结果为(81.48,1.713,0.161)。

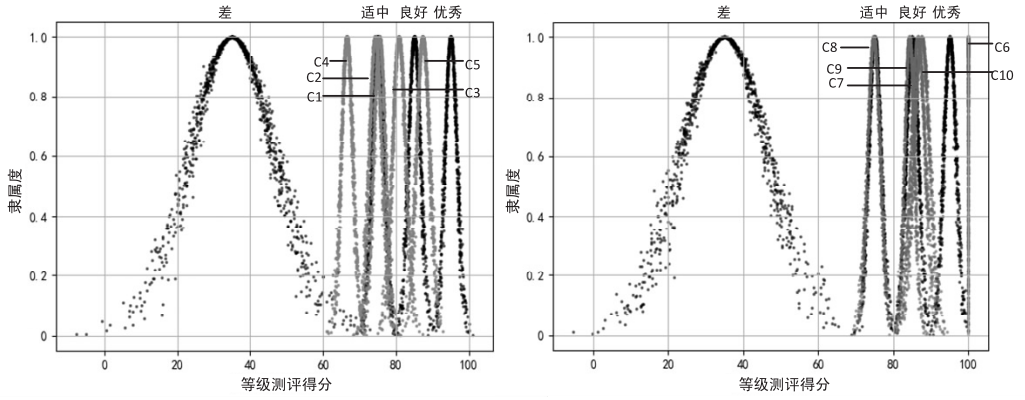
表 3　云模型特征参数

二级指标	1	2	3	4	5	6
C1	(73.5,1.833,0.183)	(75.0,1.667,0.166 7)	(74.5,1.5,0.150)	(79.5,1.833,0.183)	(77.0,1.67,0.166 7)	(73.0,1.333,0.133)
C2	(75.0,1.667,0.167)	(75.5,2.167,0.217)	(76.0,1.0,0.1)	(71.5,2.167,0.217)	(75.5,1.5,0.150)	(72.5,1.833,0.183)
C3	(79.5,2.167,0.217)	(81.5,2.167,0.217)	(81.5,1.5,0.150)	(79.0,1.667,0.167)	(81.5,1.833,0.183)	(81.5,1.5,0.150)
C4	(67.5,1.833,0.183)	(66.0,2.0,0.2)	66.5,0.833,0.083)	(67.0,2.0,0.2)	(66.0,1.333,0.133 3)	(66.0,1.0,0.1)
C5	(87.5,1.5,0.150)	(89.0,1.667,0.166 7)	(86.5,2.166 7,0.217)	(89.0,2.0,0.2)	(84.0,1.667,0.167)	(88.0,2.0,0.2)
C6	(100,0,0)	(100,0,0)	(100,0,0)	(100,0,0)	(100,0,0)	(100,0,0)
C7	(86.0,2.0,0.2)	(87.0,2.0,0.2)	(85.5,1.167,0.117)	(86.5,2.167,0.217)	(88.5,1.833,0.183)	(85.5,2.167,0.217)
C8	(76.0,2.0,0.2)	(73.0,1.667,0.167)	(75.0,1.667,0.167)	(77.5,1.5,0.150)	(74.0,2.0,0.2)	(73.0,1.333,0.133)
C9	(82.0,1.333,0.133)	(83.0,1.333,0.133)	(83.0,1.0,0.1)	(86.0,1.333,0.133)	(87.5,1.167,0.117)	(84.0,1.667,0.167)
C10	(86.5,2.167,0.217)	(88.0,2.0,0.2)	(88.0,2.333,0.233)	(86.5,2.5,0.25)	(88.0,2.0,0.2)	(88.0,1.667,0.167)

表 4 化工产业控制系统网络安全等级测评评估数据

二级指标	二级指标 云模型特征参数	一级指标	一级指标 云模型特征参数
C1	(75.41,1.649,0.164)		
C2	(74.33,1.769,0.172)		
C3	(80.75,1.827,0.181)	B1	(77.74,1.742,0.170)
C4	(66.5,1.572,0.15)		
C5	(87.33,1.848,0.183)		
C6	(100,0,0)		
C7	(86.5,1.92,0.189)		
C8	(74.75,1.712,0.169)	B2	(86.77,1.672,0.149)
C9	(84.25,1.32,0.131)		
C10	(80.75,1.827,0.181)		

绘制的评估云模型如图 3 所示,图中黑色云模型为评价衡量尺度的标准模型,灰色云模型为评价模型,都显正态分布,趋于稳定,表明该云模型有效。为了确保云模型评估的准确性,基于文献[22]中云模型相似度度量方法计算其相似度。由图可知,C = {C1,C2,C3,C4,C5,C6,C7,C8,C9,C10}的结果为{中,中,良,差,良,优,良,中,良,良},二级指标技术要求和管理要求分别为中、良,最后的综合等级测评结论位于中和良好之间且趋于良好(如图 4),根据相似度度量方法得出与良更为相似,根据最大隶属度原则,该化工工控系统综合评价等级结果为良,并且该工控系统不存在高安全风险,即该系统满足等级测评的要求,符合网络安全要求能力,该结果与预案评审结果一致,验证了该方法在网络安全等级测评中的有效性和适用性。其中安全计算环境评估结果为差,不符合网络安全等级测评要求,分析原因可知,该项在身份鉴别、安全审计、控制设备安全出现不符合情况,因此建议定期更换具有复杂度用户账号密码,审计安全事件要覆盖到每个用户,并确保需保留的控制设备应实施严格的监控管理。



(a)技术要求指标云模型 (b)管理要求指标云模型

(c)技术要求云模型 (d)管理要求云模型

图 3 技术、管理要求云模型

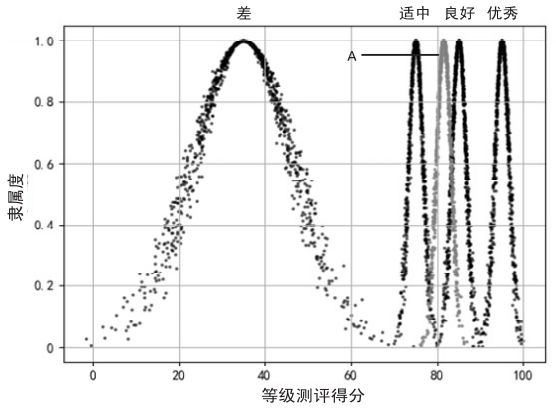


图 4　网络安全等级测评综合评估

5　结束语

网络安全等级测评可综合评判工控系统是否具备国家要求的安全保护能力,为工控系统安全防护能力的持续调优提供依据。该文构建一种网络安全等级测评评估方法,通过构建典型工控系统框架并分析其差异性,为契合工控系统等级测评提供理论支持,采用层次分析法确保工控系统评估指标权重倾斜的合理性,应用 CRITIC 法保证权重的科学性,使用组合赋权法综合考量主客观赋权优点,克服权重计算简单,缺乏工控系统权重分配合理性问题,为工控系统权重赋权提供新的方案。构建的工控系统网络安全等级测评的结果表明该方法具有良好的适用性,使用专家云模型结合组合赋权权重得出评估云特征参数,并采用云发生器绘制云图,得出网络安全等级测评评估结果,克服繁琐的计算和评估结果的模糊性问题。

参考文献:

[1] CONTI M,DONADEL D,TURRIN F. A survey on industrial control system testbeds and datasets for security research [J]. IEEE Communications Surveys & Tutorials, 2021, 23 (4):2248-2294.

[2] 唐士杰,袁　方,李　俊,等. 工业控制系统关键组件安全风险综述[J]. 网络与信息安全学报,2022,8(3):1-17.

[3] MOKHTARI S, ABBASPOUR A, YEN K K, et al. A machine learning approach for anomaly detection in industrial control systems based on measurement data[J]. Electronics, 2021,10(4):407.

[4] ZHANG D,WANG Q G,FENG G,et al. A survey on attack detection, estimation and control of industrial cyber - physical systems[J]. ISA Transactions,2021,116:1-16.

[5] BHAMARE D,ZOLANVARI M,ERBAD A,et al. Cybersecurity for industrial control systems:a survey[J]. Computers & Security,2020,89:101677.

[6] UPADHYAY D, SAMPALLI S. SCADA (supervisory control and data acquisition) systems: vulnerability assessment and security recommendations [J]. Computers & Security, 2020,89:101666.

[7] CORALLO A, LAZOI M, LEZZI M. Cybersecurity in the context of industry 4.0:a structured classification of critical assets and business impacts [J]. Computers in Industry, 2020,114:103165.

[8] 周　明,吕世超,游建舟,等. 工业控制系统安全态势感知技术研究[J]. 信息安全学报,2022,7(2):101-119.

[9] 马　力,陈广勇,张振峰,等. GB/T 22239-2019. 信息安全技术网络安全等级保护基本要求[S]. 北京:中国标准出版社,2019.

[10] 何占博,王　颖,刘　军. 我国网络安全等级保护现状与2.0 标准体系研究[J]. 信息技术与网络安全,2019,38(3):9-14.

[11] 陈广勇,李　明,黎水林,等. GB/T 28448-2019. 信息安全技术网络安全等级保护测评要求[S]. 北京:中国标准出版社,2019.

[12] 尚文利,王天宇,曹　忠,等. 工业测控设备内生信息安全技术研究综述[J]. 信息与控制,2022,51(1):1-11.

[13] 邹鑫灏,李新建,潘　伟,等. 融合网络安全等级保护系列标准的测评量化方法探讨[J]. 信息网络安全,2021(S1):190-194.

[14] 马　力. 网络安全等级保护测评中结论产生的定量计算方法研究[J]. 信息网络安全,2020,20(3):1-8.

[15] 黎水林,祝国邦,范春玲,等. 一种新的等级测评综合得分算法研究[J]. 信息网络安全,2020,20(2):1-6.

[16] 林志兴,张武威,余　建,等. 基于模糊集的高校网络安全等级保护体系研究[J]. 计算机应用与软件,2021,38(4):305-310.

[17] YU K,TAN L,MUMTAZ S,et al. Securing critical infrastructures:deep-learning-based threat detection in IIoT[J]. IEEE Communications Magazine,2021,59(10):76-82.

[18] 刘晓曼,于广琛,吴雨霖. 工控系统典型安全标准解读与思考[J]. 信息通信技术与政策,2019,45(2):40.

[19] 马　力. 网络安全等级保护测评中测评结论的度量方法优化[J]. 信息网络安全,2020,20(5):1-10.

[20] 杨元元,赵延龙. 基于组合赋权二维云模型的装配式建筑构件吊装施工安全风险评价[J]. 自然灾害学报,2022,31(3):167-174.

[21] 何永贵,刘　江. 基于组合赋权 - 云模型的电力物联网安全风险评估[J]. 电网技术,2020,44(11):4302-4309.

[22] 李海林,郭崇慧,邱望仁. 正态云模型相似度计算方法[J]. 电子学报,2011,39(11):2561-2567.