陈欣,卢海宏,薄万举.可拓方法在地震信息系统安全评价中的应用研究[J].地震工程学报,2020,42(5):1337-1342.doi:10.3969/j.issn.1000-0844.2020.05.1337

CHEN Xin,LU Haihong,BO Wanju.Application of the Extension Method to the Safety Evaluation of Seismic Information Systems[J].China Earthquake Engineering Journal,2020,42(5):1337-1342.doi:10.3969/j.issn.1000-0844.2020.05.1337

可拓方法在地震信息系统安全评价中的应用研究

陈 欣,卢海宏,薄万举

(中国地震局第一监测中心,天津 300180)

摘要:地震信息系统在地震监测预报预警、地震灾害风险防控、地震应急响应与处置等方面发挥着重要的作用,但地震行业尚未建立完整的信息系统安全评价体系,且相关研究开展较少。为了更好地识别安全风险,提高地震信息网络安全防护能力,作者利用可拓方法建立信息系统评价模型,通过程序自动进行指标权重和关联度的计算,输出系统评价等级。实例表明:可拓方法可为地震信息系统安全评价、网络安全等级保护等提供支撑,并具有应用价值。本研究为评价指标的进一步优化调整,以及自动评价软件的完善和应用提供重要的基础。

关键词:安全评价;可拓方法;地震信息系统;层次分析法

中图分类号:TP14 **文献标志码**:A **文章编号**:1000-0844(2020)05-1337-06

DOI:10.3969/j.issn.1000-0844.2020.05.1337

Application of the Extension Method to the Safety Evaluation of Seismic Information Systems

CHEN Xin, LU Haihong, BO Wanju

(*The First Monitoring and Application Center, CEA, Tianjin 300180, China*)

Abstract: Seismic information systems play an important role in earthquake monitoring and forecasting, earthquake disaster risk prevention and control, and earthquake emergency response and disposal. However, there is not a complete information security evaluation system in the seismic industry, and the related studies are few. To better identify the security risks and improve the security protection ability of seismic information networks, in this study, an information system evaluation model was established by the extension method; the index weights and correlation degree were automatically calculated through a program, and the evaluation level of the system was obtained. The examples showed that the extension method can support the security evaluation of seismic information systems and the protection of the network security level and has application value. This study provides an important basis for the further optimization and adjustment of the evaluation indexes and the improvement and application of automatic evaluation software.

Keywords: safety evaluation; extension method; seismic information system; analytic hierarchy process

收稿日期:2020-07-10

基金项目:2020 年度地震科学数据共享项目(SJGX-2020-02-02)

第一作者简介:陈 欣(1984-),女,硕士,工程师,主要从事网络安全、地震信息技术研究方面的工作。E-mail:chenxin@fmac.ac.cn。

0 引言

地震信息安全是国家网络安全的重要组成部分,关系到人民生命财产安全和防震减灾事业发展。安全体系的建立、安全性评价、风险防控成为关注的议题。一些领域的研究人员开展了相关研究[1-5],如利用神经网络[6]、模糊理论[7]等控制理论和方法研究信息系统的安全性问题,取得了一些研究成果,但上述研究也存在一些不足,且尚无地震信息系统安全性评价方面的应用研究。地震行业信息系统具有敏感性、实时性、数据量大、关注度高等特点。近年来,中国地震局发布了多个网络安全与信息化方面的文件,包括《地震信息化顶层设计》(2018 年)、《地震信息化行动方案(2018—2020 年)》(2018 年)、《中国地震局网络安全事件应急预案(试行)》(2018 年)、《地震部门网络安全等级保护定级工作指南》(2018 年)和《地震信息化建设管理办法》(2019 年)等,为地震行业信息安全各项工作的开展提供了重要的指导依据。

可拓学研究是以形式化的模型探讨事物拓展的可能性以及开拓创新的规律与方法,并用于解决矛盾问题的学科,该学科在信息系统安全风险评价研究当中具有重要的理论价值和应用前景[8-10]。本文尝试建立地震信息系统安全风险可拓评价体系,并引用合适的评价指标权重确定方法,编写程序计算指标权重和信息系统评价等级关联度,最终根据最大隶属度原则判断系统所属安全等级。该方法可以为地震信息系统安全评价工作提供新的思路,为有针对性地防控系统安全风险,提高信息系统安全防护能力提供理论基础。

1 可拓学及可拓评价方法

1.1 基本原理

可拓学自 1983 年由我国学者蔡文创立以来,历经 20 多年发展,其基本理论为可拓论,有基元理论、可拓集合理论和可拓逻辑三大支撑。其中,基元理论用物元、事元和关系元表示被研究对象;可拓集合理论对实变函数中距离的概念加以拓展,引入描述客观事物性质变化的关联函数,为表达矛盾问题的转化提供了定量手段;可拓逻辑则是辩证逻辑和形式逻辑的科学集成。[11-14]

经典的集合论认为,一个元素 v 要么属于、要么不属于某个区间$[a,b]$,没有介于二者之间的其他情况。而蔡文提出的可拓集合引入关联度表示元素 v 与区间$[a,b]$相关联的程度。现实中往往要求对多指标(各个指标权重不同)进行综合评价,得出评价等级。可拓方法针对评价等级分别计算出待评对象在该等级上的多指标带权重的关联度之和,依据最大隶属度原则,关联度之和最大者对应的等级确定为待评对象的等级。可拓方法为多指标模糊评价工作提供了一种可靠的定量分析方法[15]。

1.2 物元模型

定义基元 R 为事物的信息元:

$$R=[P,U,V]=\begin{bmatrix} P & u_1 & v_1 \\ & u_2 & v_2 \\ & \vdots & \vdots \\ & u_n & v_n \end{bmatrix} \tag{1}$$

式中:P 表示级别的全体;$U=\{u_1,u_2,\cdots,u_n\}$ 表示事物的 n 个评估指标;$V=\{v_1,v_2\cdots,v_n\}$ 表示关于评估指标的量值或者量值域。P、U、V 即为物元三要素,其反映了事物质与量的关系,客观描述系统的特性和变化过程。

1.3 经典域、节域与关联函数

设 C 为论域,若对 C 中的任一元素 $c\in C$,都有一个实数 $k(c)\in(-\infty,+\infty)$ 与之对应,则称 $\widetilde{A}=\{(c,y)\mid c\in C,y=K(c)\in(-\infty,+\infty)\}$ 为论域 C 上的一个可拓集合,其中 $y=K(c)$ 为 $\widetilde{A}$ 的关联函数。$K(c)$ 为 c 关于 $\widetilde{A}$ 的关联度。称 $A=\{F\mid F\in W,K(F)>0\}$ 为 $\widetilde{A}$ 的经典域;称 $A=\{F\mid F\in W,-1<K(F)<0\}$ 为 $\widetilde{A}$ 的节域。

经典域和节域分别为给定范围和最大范围,一般根据经验、统计或相关标准等确定[16]。

构造初等关联函数:

$$K_{ij}(v_{ij})=\begin{cases} -\rho(v_{ij},V_i), v_{ij}\in V_i \\ \dfrac{\rho(v_{ij},V_i)}{\rho(v_{ij},V_{pi})-\rho(v_{ij},V_i)}, v_{ij}\notin V_i \end{cases} \tag{2}$$

式中:$V_i=\langle a_i,b_i\rangle$ 为经典域值,$V_{pi}=\langle a_{pi},b_{pi}\rangle$ 为节域值,v_{ij} 为系统指标 i 的量值。

构建量值 v_{ij} 到经典域 V_i 和节域 V_{pi} 的可拓距公式,分别如式(3)和式(4)所示。

$$\rho(v_{ij},V_i)=\left|v_{ij}-\frac{a_i+b_i}{2}\right|-\frac{b_i-a_i}{2} \tag{3}$$

$$\rho(v_{ij},V_{pi})=\left|v_{ij}-\frac{a_{pi}+b_{pi}}{2}\right|-\frac{b_{pi}-a_{pi}}{2} \tag{4}$$

则待评价信息系统关于安全风险级别 j 的综合关联度为:

$$D_j=\sum_{i=1}^{n}\delta_i K_{ij}(j=1,2,\cdots,m) \tag{5}$$

δ_i 为指标 i 的权重。

设

$$D_{j_0}=\max_{j\in\{1,2,\cdots,m\}}D_j \tag{6}$$

根据最大隶属度原则,则该待评价系统的评价级别为 j_0。

2　地震信息系统可拓评价

2.1　评价指标的提取

根据《地震信息化建设管理办法》《地震部门网络安全等级保护定级工作指南》《信息安全等级保护管理办法》《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019),结合日常运维管理经验,我们初步设定地震信息系统五大评估指标,包括:信息安全管理制度与组织机构;安全配置;技术文档;网络架构;服务连续性评价。

将以上五大指标作为一级指标,用 U 表示:

$$U_i=[u_1,u_2,u_3,u_4,u_5]$$

再对指标进行细化,引入二级指标,共 18 个评价指标,如图 1 所示,即指标权重模型由评价对象、一级指标和二级指标组成。

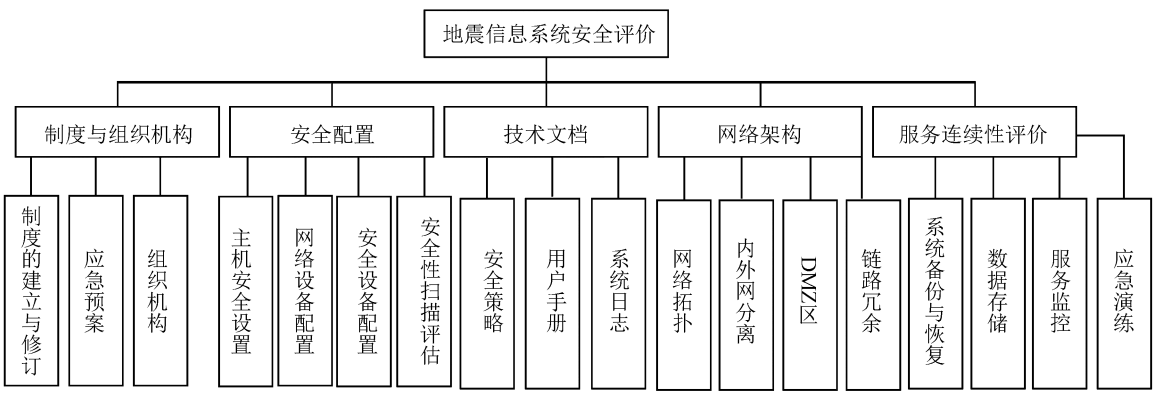

图 1　地震信息系统安全评价指标层次结构模型

Fig.1　Hierarchical model of security evaluation indicators for seismic information systems

2.2　确定指标权重系数

系统的每个评价指标对于地震信息系统安全风险评估的重要程度不同,以权重描述其重要程度,不同权重系数很大程度上会影响评价结果,权重系数的取值对于系统安全评价科学性具有十分重要的作用。权重的确定方法有排序打分法、简单关联法、层次分析法等,其中层次分析法对各指标之间重要程度的分析更具有逻辑性,加上数学处理,可信度较大。

2.2.1　构建判断矩阵

为了确定各个指标对信息系统安全评价的重要程度即权重,通过在各层指标中对每个指标两两进行量化比较,构造出判断矩阵:

$$A=\begin{bmatrix}\frac{W_1}{W_1} & \frac{W_1}{W_2} & \cdots & \frac{W_1}{W_n}\\ \frac{W_2}{W_1} & \frac{W_2}{W_2} & \cdots & \frac{W_2}{W_n}\\ \vdots & \vdots & & \vdots\\ \frac{W_n}{W_1} & \frac{W_n}{W_2} & \cdots & \frac{W_n}{W_n}\end{bmatrix} \tag{7}$$

式中:W_m 表示第 m 个指标对应于上一层次中指标的重要性的权重。设 $a_{mn}=W_m/W_n$,则 a_{mn} 具有以下性质:

(1) $a_{mn}=1$ $(m=n;m,n=1,2,\cdots,n)$;

(2) $a_{mn}=1/a_{nm}(m\neq n;m,n=1,2,\cdots,n)$

按照 9/9 ~ 9/1 标度法对信息系统安全评价的 5 个一级指标影响因素进行两两比较后构成判断矩阵如式(8):

$$A=\begin{bmatrix}1 & \frac{3}{9} & \frac{5}{9} & \frac{3}{9} & \frac{7}{9}\\ \frac{9}{3} & 1 & \frac{9}{7} & 1 & \frac{9}{7}\\ \frac{9}{5} & \frac{7}{9} & 1 & \frac{7}{9} & 1\\ \frac{9}{3} & 1 & \frac{9}{7} & 1 & \frac{9}{7}\\ \frac{9}{7} & \frac{7}{9} & 1 & \frac{7}{9} & 1\end{bmatrix} \tag{8}$$

2.2.2　计算权重系数

由于一致性矩阵具有这样一条性质:

若 A 的最大特征值 $\lambda_{\max}$ 对应的特征向量为 $W=(w_1,\cdots,w_q)^T$,则 $a_{mn}=\frac{w_m}{w_n}$。

根据这条性质可知通过求判断矩阵的最大特征值所对应的特征向量，并做归一化处理，就可以获得各个指标的权重 w_i。

用 MATLAB 程序计算出最大特征值对应的特征向量 W 为

$$W=[0.224\ 2,0.560\ 5,0.412\ 2,0.560\ 5,0.389\ 3]^T$$

做归一化处理得到每个一级指标影响因素的权重系数：

$$\delta_i=[0.104\ 5,0.261\ 1,0.192\ 0,0.261\ 1,0.181\ 3]$$

然后我们对矩阵进行一致性验证，矩阵 A 的最大特征值 $\lambda_{max}=5.038\ 7$，满足一致性要求。

同理，分别构造各个一级指标下的二级指标判断矩阵，并进行一致性检验，得到二级指标的权重系数，分别为

$$\delta_b=[0.031\ 8,0.040\ 9,0.031\ 8],$$

$$\delta_c=[0.130\ 6,0.043\ 5,0.056\ 0,0.031\ 1],$$

$$\delta_d=[0.082\ 3,0.045\ 7,0.064\ 0],$$

$$\delta_e=[0.146\ 9,0.049\ 0,0.038\ 1,0.027\ 2],$$

$$\delta_f=[0.051\ 7,0.089\ 3,0.014\ 7,0.025\ 6]$$

综上，18 个二层评价指标的权重如表 1 所列。

表 1 权重系数表

Table 1 Table of weighting factors

编号	安全指标	权重	编号	安全指标	权重
1	制度的执行与修订	0.031 8	10	系统日志	0.064 0
2	应急预案	0.040 9	11	网络拓扑	0.146 9
3	组织机构	0.031 8	12	内外网分离	0.049 0
4	主机安全设置	0.130 6	13	DMZ 区	0.038 1
5	网络设备配置	0.043 5	14	链路冗余	0.027 2
6	安全设备配置	0.056 0	15	系统备份与恢复	0.051 7
7	安全性扫描评估	0.031 1	16	数据存储	0.089 3
8	安全策略	0.082 3	17	服务监控	0.014 7
9	用户手册	0.045 7	18	应急演练	0.025 6

2.3 确定评价级别的经典域和节域

我们先将系统安全等级分为四级，即：

$$G_j=\{G_1,G_2,G_3,G_4\}=\{优,良,及格,不及格\}$$

其中，明确四个级别的对应分值范围分别是：优[90,100]、良[80,90)、及格[60,80)、不及格[0,60)。

由此，我们将系统安全信息元描述为：

$$R_j=[P_j,U_i,V_j]=\begin{bmatrix} P_j & u_1 & V_{1j} \\ & u_2 & V_{2j} \\ & u_3 & V_{3j} \\ & u_4 & V_{4j} \\ & u_5 & V_{5j} \end{bmatrix} \tag{9}$$

$U_i=[u_1,u_2,u_3,u_4,u_5]$ 为 5 个一级评价指标；$P_j(j=1,2,3,4)$ 为地震信息系统安全风险的 4 个级别；$V_{ij}=[0,100]$ 为 P 关于 u_i 的取值范围，即 P 的节域。

将 4 个级别对应的分值范围代入信息元：

$$R_0=\begin{bmatrix} G & G_1 & G_2 & G_3 & G_4 \\ U & V_1 & V_2 & V_3 & V_4 \end{bmatrix}=$$

$$\begin{bmatrix} G & G_1 & G_2 & G_3 & G_4 \\ u_1 & [90,100] & [80,90) & [60,80) & [0,60) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ u_5 & [90,100] & [80,90) & [60,80) & [0,60) \end{bmatrix}$$

其中，区间 v_{ij} 分别为 G_j 关于指标 u_i 所规定的量值范围，即经典域。

2.4 计算关联度

由专家结合相关设计验收文档的检查、调查访谈等，给出待评价各个指标的分值。

某地震信息系统安全量化评分表如表 2 所列。

表 2 某地震信息系统安全量化评分表

Table 2 Quantitative safety score sheet for a seismic information system

编号	安全指标	评分	编号	安全指标	评分
1	制度的执行与修订	90	10	系统日志	83
2	应急预案	90	11	网络拓扑	89
3	组织机构	95	12	内外网分离	60
4	主机安全设置	90	13	DMZ 区	70
5	网络设备配置	85	14	链路冗余	85
6	安全设备配置	85	15	系统备份与恢复	80
7	安全性扫描评估	80	16	数据存储	83
8	安全策略	90	17	服务监控	75
9	用户手册	92	18	应急演练	50

设 k_{ij} 为考虑指标权重的基础上被评价系统关于等级 j 的关联度，根据式(2)～(4)，利用 MATLAB 程序计算 $k_{i1}(i=1,2,\cdots,18)$ 并加权求和即为被测系统针对第一等级关联度 D_1。同理，依次算出被测系统与四个等级的关联度：

$D_j=[-0.144\ 32, 0.061\ 082, -0.296\ 39, -0.604\ 59]$

2.5　系统等级评价

根据式(6)，计算出级别变量特征值为 1.89，则该地震信息系统评级为第 2 级“良”。信息系统可参考专家评分汇总表整改薄弱指标项，提高系统安全性。

本文所有的计算步骤均可通过程序实现，并且完成评价软件的初步设计开发，如图 2 所示。

图 2　地震信息系统评价软件

Fig.2　Evaluation software for the seismic information system

3　讨论

主要讨论信息系统安全性的评价体系和方法，在指标的选择上，从信息安全管理者的角度选择了具有代表性的指标，从判断矩阵一致性等方面考察证明这些指标具有可用性，同时这些指标可以根据实际情况进一步验证和完善，单项否决项的程序实现需要在后续研究中进行补充。

将地震信息系统可拓评价方法进行了梳理和应用研究，并将计算步骤和评价过程通过程序实现。后续研究中继续完善自动评价软件，使评价过程更具适应性，更加简单、便捷。

4　结语

系统阐述可拓方法在地震信息系统安全评价中的应用和实施过程，为其今后的广泛应用打下基础。根据实例结果，得到如下结论：

(1) 可拓评价方法可以较好的应用于地震信息系统安全评价当中；

(2) 作者将可拓评价方法通过程序实现，可实现一定程度上的自动评价；

(3) 根据地震信息系统的特点和实际情况，可以从多个角度入手对可拓评价方法和自动评价软件进行进一步完善和优化。

参考文献(References)

[1] 傅钰.网络安全等级保护 2.0 下的安全体系建设[J].网络安全技术与应用，2018(8)：13-13，16.
FU Yu. Net Security Technologies and Application，2018(8)：13-13，16.

[2] 李钊，徐国爱，班晓芳，等.基于元胞自动机的复杂信息系统安全风险传播研究[J].物理学报，2013，62(20)：10-19.
LI Zhao，XU Guo'ai，BAN Xiaofang，et al. Complex Information System Security Risk Propagation Research Based on Cellular Automata[J]. Acta Physica Sinica，2013，62(20)：10-19.

[3] 鲁县华.民航空管系统安全评估技术研究[D].天津：天津大学，2012.
LU Xianhua. Research on safety assessment technology of civil aviation air traffic control system. Tianjin：Tianjin University，2012.

[4] 王丰，张春平，林瑜，等.军事院校信息系统安全风险的可拓识别评估[J].武汉理工大学学报(信息与管理工程版)，2018，40(6)：606-609.
WANG Feng，ZHANG Chunping，LIN Yu，et al. Extension Identification and Evaluation of Information System Security Risk in Military Academy[J]. Journal of Wuhan University of Technology (Information & Management Engineering)，2018，40(6)：606-609.

[5] 吴晨，董吉文，房晓亮，等.地震行业信息安全体系建设[J].地震地磁观测与研究，2013，34(3)：245-251.

WU CHEN,DONG Jiwen,FANG Xiaoliang,et al.Earthquake Profession Information Security System Construction Research [J].Seismological and Geomagnetic Observation and Research,2013,34(3):245-251.

[6] 王海燕.基于 GRA-RBF 神经网络的信息安全风险评价[J].内蒙古师范大学学报(自然科学汉文版),2016,45(2):166-169,173.
WANG Haiyan.Information Security Risk Assessment Model Based on GRA-RBF Neural Network[J].Journal of Inner Mongolia Normal University (Natural Science Edition),2016,45(2):166-169,173.

[7] 王帆,霍明奎,王晓婷.基于模糊灰度的信息系统安全风险评价与对策[J].情报科学,2014,32(1):110-114.
WANG Fan, HUO Mingkui, WANG Xiaoting. Information System Security Risk Assessment Based on the Fuzzy Gray-level and Countermeasures[J]. Information Science, 2014, 32(1):110-114.

[8] CAI WEN,YANG CHUNYAN,ZHAO YAN,et al.New Development of the Basic Theory of Extenics[J].Engineering Sciences,2004(01):40-45.

[9] 杨春燕,蔡文.可拓学[M].北京:科学出版社,2014:70-170.
YANG Chunyan, CAI Wen. Extenics [M]. Beijing: Science Press,2014:70-170.

[10] 薛晓锋.斜拉桥拉索阻尼器的选型评价[D].西安:长安大学,2010:81-90.
XUE Xiaofeng.Selection and Evaluation of Cable Dampers for Cable Stayed Bridges[D].Xi'an:Changan University,2010:81-90.

[11] 蔡文.可拓集合和不相容问题[J].科学探索学报,1983,(1).
CAI Wen. Extension Set and Incompatibility Problem [J]. Journal of Scientific Exploration,1983,(1).

[12] 蔡文.物元模型及其应用[M].北京:科学技术文献出版社,1994.
CAI Wen.Matter Element Model and Its Application[M].Beijing:Science and Technology Literature Press,1994.

[13] 蔡文.从物元分析到可拓学[M].北京:科学技术文献出版社,1995.
CAI Wen. From Matter Element Analysis to Extenics[M]. Beijing:Science and Technology Literature Press,1995.

[14] 蔡文,杨春燕,林伟初.可拓工程方法[M].北京:科学出版社,1997.
CAI Wen,YANGChunyan,LIN Weichu.Extension Engineering Method[M].Beijing:Science Press,1997.

[15] 刘智慧.可拓方法在信息安全评价中的应用[J].电力信息化,2004,2(9):41-42.
LIU Zhihui.Application of Extension Method in Information Security Evaluation.[J].Electric Power Information Technology,2004,2(9):41-42.

[16] 蔡文,杨春燕,陈文伟.可拓集与可拓数据挖掘[M].北京:科学出版社,2008.
CAI Wen,YANGChunyan,CHEN Wenwei.Extension Set and Extension Data Mining[M].Beijing:Science Press,2008.