基于模糊综合评判理论的电力信息系统安全风险评估模型及应用

梁丁相[1]，陈 曦[2]

（1.宁夏回族自治区固原市供电局，宁夏 固原 756000；2.河北保定供电公司，河北 保定 071000）

摘要：提出一种基于模糊综合评判理论的信息系统安全风险综合评估模型与方法，实现量化信息系统安全风险的目标。通过确定信息系统的安全风险因素集、指标集以及因素的权重系数集，建立安全风险模糊综合评估矩阵，并应用于电力信息系统Web组件的安全风险评估。电力信息系统受到来自系统本身、外部环境以及人为和自然界的安全威胁，应用建立的信息系统安全风险评估模型定量计算电力信息系统Web组件的安全风险值，为系统管理与使用部门采取相应的防护技术和管理措施提供理论依据。

关键词：电力信息系统；信息系统安全；风险评估；模糊数学

Safety assessment model of electric power information system based on fuzzing synthetical theory and its application

LIANG Ding-xiang[1]， CHEN Xi[2]

(1.Guyuan Power Supply Company，Guyuan 756000， China；

2.Baoding Power Supply Company，Baoding 071000，China)

Abstract: A safety assessment model of electric power information system based on fuzzing theory is proposed to implement the goal of quantizing information system safety assessment. Assessing matrix is established based on fuzzing synthetical theory by building assemble of power information system safety element and its weight coefficient and index assemble. And the matrix is applied to the power system. Electric power information system is influenced by circumstance, artificial and natural factors. By using this model to calculate electric power system WEB component value of risk, supplying theory gist for information system managing and operating department.

Key words: information system of electric power system; safety of information system; risk assessment; · fuzzy mathematics

中图分类号：TM73 文献标识码：A 文章编号：1674-3415(2009)05-0061-04

0 引言

随着电力信息化的快速发展，计算机网络与信息技术在电力行业得到了广泛应用。各电力企业建立了涵盖生产、管理及营销等各个环节的应用系统，网络与信息系统的基础性、全局性作用日益增强，但网络与信息安全的问题也随之而来，网络与信息安全已成为电力安全生产的重要组成部分。在电力企业的综合信息管理系统中，必须从网络、操作系统、应用程序和业务需求等各方面来保证系统的安全，提高信息系统整体安全水平。本文提出一种基于模糊综合评判理论的信息系统安全风险综合评估模型与方法，对电力信息系统中Web组件的安全性进行风险评估，量化安全风险。

1 信息系统安全风险综合评估模型

信息系统安全风险评估[1,2]是指依据有关信息安全技术与管理标准,对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。信息系统的安全风险与资产、威胁、脆弱性这三大要素相关。其中，威胁是触发信息系统安全风险的主导因素，而信息系统面临的威胁分为人为的威胁和自然的威胁。人为的威胁包括偶然的人为操作失误、蓄意的计算机网络攻击行为；自然的威胁包括火灾、地震、飓风等环境因素，硬件故障等等，这些威胁因素对信息系统安全风险影响是不确定的,具有模糊性。基于模糊综合评判理论的信息系统安全风险评估[3~5],是通过专家经验赋予每种威胁风险指标值,利用模糊评估矩阵运算,获

得量化的信息系统安全风险的严重程度,对影响信息系统安全性的多种风险因素做出总体评价。

1.1 确定系统的安全风险因素集

设 S 为信息系统的所有安全风险因素集，将性质相近的因素分在一组，假定 S 中的因素分为 1 组，即：

$$S=\{S_1,S_2,S_3,\cdots,S_l\} \tag{1}$$

式中：S_i 代表 S 中的第 i 组因素，i=1，2，…，l，$S=\bigcup_{i=1}^{l} S_i$。

针对每个 S_i 有 n 个风险因素集，表示成 $S_i=\{s_{i1},s_{i2},s_{i3},\cdots,s_{in}\}$ 这样，将安全风险因素集合分为多层次集合。

1.2 定义安全风险指标

安全风险指标 V，表示信息系统安全风险发生时产生的后果对信息系统的影响程度。

$$V=\{v_1,v_2,v_3,\cdots,v_m\} \tag{2}$$

式中：m 表示风险指标集的数目；vj 表示安全风险指标，j=1,2,…,m。

1.3 确定安全风险因素的权重系数

S_i 中各个因素相对安全风险指标集 V 的权重。系数用矩阵表示为

$$A_i=[a_{i1},a_{i2},a_{i3},\cdots,a_{in}] \tag{3}$$

式中：$a_{i1}+a_{i2}+a_{i3}+\cdots+a_{in}=1$，$a_{in}$ 依据 S_i 中各因素对安全风险影响的严重程度而定。

1.4 计算安全风险综合评估矩阵

首先确定单因素 s_{in} 相对安全风险指标集 V 的单因素模糊评估矩阵 $\boldsymbol{R}_i$ 即

$$\boldsymbol{R}_i=[r_{i1},r_{i2},r_{i3},\cdots,r_{in}] \tag{4}$$

式中：$r_{i1}+r_{i2}+r_{i3}+\cdots+r_{in}=1$；$r_{ij}$ 表示安全风险指标 v_j 在安全风险因素子集 S_i 的因素 s_{in} 中所占的百分比。利用符合运算求安全风险因素子集 S_i 的综合评估矩阵 $\boldsymbol{B}_i$：

$$\boldsymbol{B}_i=\boldsymbol{A}_i\circ\boldsymbol{R}_i=[b_{i1},b_{i2},b_{i3},\cdots,b_{in}] \tag{5}$$

式中：

$$b_{ij}=\sum_{k=1}^{n}(a_{ij}r_{ij});\quad 1\le j\le m \tag{6}$$

然后,确定高层因素 S 的安全风险模糊综合评估矩阵 $\boldsymbol{B}$。

$$\boldsymbol{B}=\begin{bmatrix}\boldsymbol{B}_1\\ \boldsymbol{B}_2\\ \vdots\\ \boldsymbol{B}_l\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}_1\circ\boldsymbol{R}_1\\ \boldsymbol{A}_2\circ\boldsymbol{R}_2\\ \vdots\\ \boldsymbol{A}_l\circ\boldsymbol{R}_l\end{bmatrix}_{l\times m} \tag{7}$$

最后,计算综合各种安全风险因素的安全风险 S。

$$S=\boldsymbol{B}\boldsymbol{V}^{\mathrm{T}} \tag{8}$$

2 威胁电力信息系统安全主要因素

2.1 电力信息系统资产

电力信息系统[6~8]需要保护的资产包括信息资产和物理资产两部分：

(1) 物理资产。包括系统中的各种软、硬件和物理设施。硬件资产包括计算机、交换机、集线器、网关设备等网络设备；软件资产包括计算机操作系统、网络操作系统、通用应用软件、网络管理软件、数据库管理软件和业务应用软件等。物理设施包括场地、机房、以及防水、防火、地震、雷击等的灾难应急等设施。

(2) 信息资产。包括系统业务信息、系统维护管理信息。系统业务信息包括调度、计划等业务应用数据。系统维护管理信息包括系统运行、系统监督日志、入侵检测记录、系统口令、系统权限设置、数据存储分配、IP 地址分配信息等等。

2.2 电力信息系统面临的威胁

根据威胁的不同来源,系统主要面临的安全威胁分为以下 4 类。

(1) 信息系统自身的安全脆弱性和缺陷带来的安全风险。信息系统的安全脆弱性和缺陷来自于组成信息系统的硬件的物理安全缺陷、软件组件(包括操作系统、应用平台和应用业务)的设计漏洞、功能冗余、逻辑混乱，以及网络通信协议功能完备性、可靠性和可控性方面的安全隐患。

(2) 来自内部的安全威胁。绝大多数的恶意攻击是来自内部的，原因诸多且复杂，如系统管理员失职、操作人员的失误、内部不满分子的恶意攻击等。恶意攻击的手段很多，诸如尝试使资源拒绝服务、窃听、窃取信息、伪装合法用户或系统进程、修改信息内容、利用支持系统弱点、恶意代码、伪造合法系统服务、恶意泄密、黑客技术、病毒等等，但目的无外乎窃密和破坏。

(3) 来自外部环境的安全威胁。不管企业内部的组网方式如何，通过 Internet 网络对企业内部网络构成的安全威胁却总是存在的。黑客、间谍或其他犯罪分子可以采取搭线窃听、网络监听、网络扫描等手段截取信息，存在一定的安全隐患，需要防范。另外从管理上应杜绝外部人员接触、使用电力信息系统的终端设备。

(4) 来自自然界的安全威胁。包括洪水、飓风、地震等自然灾害可能引起系统的暂停或服务中断。

3　信息系统安全风险评估实例

以电力信息系统的 Web 服务器为例,利用建立的综合评估模型,综合计算评估 Web 服务器的安全风险。影响 Web 服务器安全的风险因素 S 包括 5 组，即：$S=\{S_1,S_2,S_3,S_4,S_5\}$={数据库管理系统，Web 服务器操作系统，Web 服务器应用系统，硬件，通信设备}。

这 5 组风险因素分别由以下风险因素组成：

$S_1=\{S_{11},S_{12},S_{13},S_{14}\}$={数据文件遭到破坏,查询或恢复过程出错,数据修改出错,删除出错}

$S_2=\{S_{21},S_{22},S_{23},S_{24},S_{25}\}$={缓冲区溢出,寄存器遭到破坏，文件及目录结构破坏，用户帐户及优先权重写，不同应用程序之间冲突}

$S_3=\{S_{31},S_{32},S_{33},S_{34}\}$={功能错误，不能访问所需的资源，非法数据输入，与操作系统版本冲突}

$S_4=\{S_{41},S_{42},S_{43},S_{44},S_{45}\}$={内存出现故障，CPU 出现故障，硬件驱动出现故障，电源出现故障，总线出现故障}

$S_5=\{S_{51},S_{52},S_{53}\}$={网络硬件或接口出现故障，通信协议出现现故障，路由器故障}。

根据专家的专业知识和经验，针对上述五组风险因素，分别确定信息系统安全相对风险指标的权重系数，如下：

$\boldsymbol{A}_1$=[0.4，0.2，0.2，0.2]

$\boldsymbol{A}_2$=[0.25，0.2，0.2，0.1]

$\boldsymbol{A}_3$=[0.3，0.2，0.3，0.2]

$\boldsymbol{A}_4$=[0.25，0.3，0.2，0.1]

$\boldsymbol{A}_5$=[0.4，0.2，0.4]

通过对信息系统的开发、使用、维护和管理人员进行信息安全风险问卷调查，根据专家的专业知识和经验，利用德尔菲法对指标体系进行分析、判断并主观赋权值。当专家意见分歧程度局限在 5%~10% 时停止调查。并对获得的数据进行归一化处理,从而确定模糊评估矩阵，如下：

$$\boldsymbol{R}_1=\begin{bmatrix}0.49 & 0.34 & 0.71\\ 0.13 & 0.25 & 0.62\\ 0.26 & 0.42 & 0.32\\ 0.28 & 0.31 & 0.41\end{bmatrix}$$

$$\boldsymbol{R}_2=\begin{bmatrix}0.64 & 0.28 & 0.08\\ 0.56 & 0.32 & 0.12\\ 0.18 & 0.29 & 0.53\\ 0.23 & 0.45 & 0.32\\ 0.31 & 0.47 & 0.22\end{bmatrix}$$

$$\boldsymbol{R}_3=\begin{bmatrix}0.37 & 0.42 & 0.21\\ 0.59 & 0.33 & 0.08\\ 0.14 & 0.55 & 0.31\\ 0.23 & 0.57 & 0.20\end{bmatrix}$$

$$\boldsymbol{R}_4=\begin{bmatrix}0.53 & 0.38 & 0.09\\ 0.27 & 0.35 & 0.38\\ 0.29 & 0.22 & 0.49\\ 0.18 & 0.24 & 0.58\\ 0.41 & 0.36 & 0.23\end{bmatrix}$$

$$\boldsymbol{R}_5=\begin{bmatrix}0.32 & 0.44 & 0.24\\ 0.29 & 0.62 & 0.09\\ 0.47 & 0.49 & 0.04\end{bmatrix}$$

根据式(6)运算得：

$\boldsymbol{B}_1$=[0.330,0.332,0.338]

$\boldsymbol{B}_2$=[0.3965，0.3515，0.2520]

$\boldsymbol{B}_3$=[0.317，0.471，0.172]

$\boldsymbol{B}_4$=[0.3395，0.3160，0.3445]

$\boldsymbol{B}_5$=[0.374，0.456，0.130]

根据式(7)运算得：

$\boldsymbol{B}$=[0.35158，0.38168，0.25275]

归一化为：

$\boldsymbol{B}'$=[0.35657，0.38709，0.25634]

设定风险指标集为：

$\boldsymbol{V}$=[0.23, 0.64, 0.13]

根据式(8)运算可得风险值为：

$$\boldsymbol{S}=\boldsymbol{B}\boldsymbol{V}^{\mathrm{T}}=\begin{bmatrix}0.35657 & 0.38709 & 0.25634\end{bmatrix}\begin{bmatrix}0.23\\ 0.64\\ 0.13\end{bmatrix}=$$

0.36307

即在电力信息系统运行过程中,当 Web 服务器发生安全故障时，对系统安全影响为 0.363 07。同理，可以计算工作站或数据库等系统组件的安全风险值。安全风险值较大的关键组件应引起系统管理与使用部门的关注，并采取相应的防护技术和管理措施，增强系统的安全性。

4　结论

电力信息系统包括信息资产和物理资产，受到来自系统本身、外部环境以及人为和自然界的安全威胁。本文提出一种基于模糊数学理论的信息安全风险评估模型，应用该模型定量计算电力信息系统组件的安全风险值，为系统管理与使用部门采取相

应的防护技术和管理措施提供理论依据,对于增强系统安全性有一定的实用价值。

参考文献

[1] 戴宗坤，罗万伯，唐三平,等.信息系统安全[M]. 北京：金城出版社，2000.
DAI Zong-kun, LUO Wan-bo, TANG San-ping, et al. Safety of Information System[M]. Beijing: JINCHENG Publishing Company,2000.

[2] 关义章，蒋继红，方关宝,等. 信息系统安全工程学[M]. 北京：金城出版社，2000.
GUAN Yi-zhang, JIANG Ji-hong, FANG Guan-bao, et al. Safe Engineering Science of Information System[M]. Beijing: JINCHENG Publishing Company,2000.

[3] 汪培庄.模糊系统理论与模糊计算机[M].北京:北京科学出版社,1996.
WANG Pei-zhuang. Fuzzy System Theory and Fuzzy Computer[M]. Beijing: Science Publishing Company of Beijing,1996.

[4] 张李义.信息系统开发的动态风险模糊估测方法[J].系统工程理论与实践,2001,21(10):88-92.
ZHANG Li-yi. Safety Assessment of Information System Development[J]. Theory and Practice of System Engineering, 2001,21(10):88-92.

[5] 李洪兴.工程模糊数学及应用[M].天津:天津科学技术出版社, 1993.
LI Hong-xing. Engineering Fuzzy Mathematics and Its Application[M]. Tianjin: Technology Publishing Company of Tianjin,1993.

[6] 伍晓平. 电力信息应用系统的安全性建设[J]. 电力信息化，2004, 2(7)：55-58.
WU Xiao-ping. Security Construction of Electric Power Information System[J]. Electric Power Information, 2004, 2(7)：55-58.

[7] 余勇，林为民. 电力信息系统安全保障体系[J].电力信息化, 2003, 1(3)：58-60.
YU Yong, LIN Wei-min. Guarantee System of Electric Power System[J].Electric Power Information,2003, 1(3)：58-60.

[8] 李鹤田,刘 云,何德全. 信息系统安全工程可靠性的风险评估方法[J]. 北京交通大学学报, 2005, 29(2)：62-64.
LI He-tian，LIU Yu, HE De-quan. Security Accessment of Information System Safety[J]. Transaction of Beijing Jiaotong University, 2005, 29(2)：62-64.

收稿日期：2008-05-05；　修回日期：2008-07-02

作者简介：

梁丁相(1969-)，男，大学本科，工程师，从事变电运行工作；E-mail:protectiverelay@163.com

陈　曦（1981-），女，工学硕士，研究方向为电力系统分析、运行与控制，目前主要从事电力系统自动化工作。

（上接第 36 页　continued from page 36）

[5] 李习武，王艳松.基于小波神经网络的电能质量扰动辨识[J].电气技术，2007,9(9):56-58.
LI Xi-wu, WANG Yan-song. Recognition of Power Quality Disturbances Based on Wavelet Network[J]. Electrical Engineering, 2007,9(9):56-58.

[6] Gaing Zwe-Lee Wavelet-based Neural Network for Power Disturbance Recognition and Classification Power Delivery[J]. IEEE Trans on Publication Date,2004,(19):4.

[7] 赵凤展，杨仁刚.基于时域、小波变换和FFT的电能质量扰动识别[J].继电器,2006,4(8):50-55.
ZHAO Feng-zhan, YANG Ren-gang. Power Quality Disturbances Classification Based on Time-domain,Wavelet Transform and FFT[J]. Relay, 2006,4(8):50-55.

[8] Malabika B, Biswajit B. Analysis of Power Quality (PQ) Signals by Continuous Wavelet Transform[A]. In: Power Electronics Specialists Conference[C]. 2007.

[9] 程浩忠,艾芊,张志刚, 等. 电能质量[M]. 北京:清华大学出版社，2009.
CHENG Hao-zhong, AI Qian, ZHANG Zhi-gang, et al. Power Quality[M]. Beijing: Tsinghua University Press, 2009.

[10] 李健平，杨万年.小波十讲[M]. 北京:国防工业出版社, 2004.
LI Jian-ping,YANG Wan-nian.Ten Lectures on Wavelets[M]. Beijing: Defense Industry Press, 2004.5.

[11] 吕新华，何川平，李早华，等.一种长序列小波变换快速算法的DSP实现[J]. 现代电子技术，2008,(9):132-134.
Lü Xin-hua,HE Chuan-ping, LI Zao-hua, et al. Implementation of Long Sequence Wavelet Transform Based on DSP[J]. Modern Electronics Technique, 2008,(9):132-134.

收稿日期：2008-04-21；　修回日期：2008-07-29

作者简介：

储　珺（1983-），男,硕士，电力电子与电力传动专业，研究方向为电能质量分析; E-mail: chujun007@126.Com

马建伟（1965-），男,博士，副教授，研究方向为多变量控制理论、电能质量分析方面的研究。