第 43 卷 第 11A 期
2016 年 11 月
计 算 机 科 学
Computer Science
Vol. 43 No. 11A
Nov 2016

结合 OWA 算子和模糊 DEMATEL 的风险评估方法

林晓华 贾文华
(南京工程学院机械工程学院 南京 211167)

摘 要 针对传统故障模式与影响分析(FMEA)方法在实际应用中的不足,提出一种基于有序加权平均(OWA)算子和决策试行与评价实验法(DEMATEL)的风险排序方法。FMEA 专家对故障模式的 3 个风险因子给出模糊评价信息,应用 OWA 算子对评估信息进行集结,得到各故障原因对故障模式的影响强度。采用模糊 DEMATEL 法构建 FMEA 系统要素间的初始直接影响矩阵,经过运算可得综合影响矩阵,并计算各故障原因的原因度,据此进行产品或系统的失效风险评估。运用该方法对地铁车门系统的基础部件进行安全性分析,并将所得结果与传统 RPN 方法的结果做对比,验证了该方法的可行性和有效性。

关键词 故障模式与影响分析(FMEA),风险评估,模糊数,OWA 算子,DEMATEL 法
中图法分类号 TH122 **文献标识码** A

FMEA Method Combining OWA Operator and Fuzzy DEMATEL

LIN Xiao-hua JIA Wen-hua
(School of Mechanical Engineering, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract Considering the shortcomings of traditional failure mode and effect analysis(FMEA) method in practical application, a risk ranking method was proposed based on ordered weighted averaging(OWA) operator and decision making trial and evaluation method(DEMATEL). FMEA experts make fuzzy evaluation on the three risk factors of the failure modes, and the evaluation information is aggregated by OWA operator to get the influence degree of the failure cause to failure mode. The initial direct-relation fuzzy matrix of the FMEA system is constructed by using fuzzy DEMATEL method, then the total-relation fuzzy matrix is calculated, and the reason degree of each failure cause is computed, based on which the product or system risk assessment is conducted. The proposed method is applied to safety analysis of the basic components of the metro car door system, and the feasibility and effectiveness of the method is verified by comparing with the results of the traditional RPN method.

Keywords Failure mode and effect analysis(FMEA), Risk assessment, Fuzzy number, OWA operator, DEMATEL method

故障模式与影响分析(Failure Mode and Effects Analysis, FMEA)是一种自底向上的系统安全性分析方法,通过具体工艺过程或零部件潜在故障模式和原因的分析,判断其可能会对过程或产品造成的影响(即风险程度),据此提出针对性的预防或改进措施,以提高过程或产品的质量和可靠性。该方法被广泛应用于航空、核工业、电子、机械以及医疗等领域[1-4]。

FMEA 分析通常采用风险优先数(Risk Priority Number, RPN)方法进行定量分析,首先要确定产品或系统的潜在故障模式,然后分析各故障模式的发生度(Occurrence, O)、严重度(Severity, S)和难测度(Detection, D)。RPN 等于 O,S,D 的乘积,按照 RPN 值对故障模式进行排序,根据排序决定预防和改进措施的优先次序。RPN 值越大表明其对应的故障模式的风险越大,造成的后果越危险,就应当给予更多的关注。然而随着实践应用,该方法的不足之处也不断显现,具体如下:

(1)O,S,D 3 个风险因子被视为同等重要,未考虑 O,S,D 的相对重要性。事实上,不同的 O,S,D 数值的乘积可以得到相同的 RPN 值,那么据此判断其对应的故障模式就会是同等风险的,而事实上其潜在的风险可能相差不小。如此,分析结果就可能造成资源、时间的浪费,更甚至未能及时察觉潜在风险很大的故障模式。

(2)对于 3 个风险因子 O,S,D 的评价,往往难以给出精确的数值。FMEA 分析中涉及的很多信息具有模糊性、不确定性;而另一方面,人们也习惯使用定性模糊语言来描述,但传统方法在处理模糊信息时存在局限性,从而导致 FMEA 的应用受到限制。

(3)多数情况下,引发产品或系统故障模式的原因有很多,它们之间存在一定的关联,传统 RPN 法未能考虑这种关联影响,就会导致分析结果出现偏差。比如当一个原因可以引发多个故障模式时,在采取预防或改进措施时就应当给予更高的优先级。

本文受国家自然科学基金(51505211),江苏省自然科学青年基金(BK20130741),南京工程学院引进人才科研启动基金(YKJ201301)资助。
林晓华(1985-),女,博士,讲师,主要研究方向为产品设计理论及方法、产品质量控制,E-mail:zdlxh5001@163.com。

针对传统方法的缺点，国内外专家学者作了一些改进研究。Zhou 等[5]应用模糊集理论计算故障模式的模糊 RPN 值，并运用灰色理论计算系统的灰色关联系数，故障模式的排序取决于模糊 RPN 和灰色关联系数；Lolli 等[6]引入多准则决策方法来解决故障模式间的关联问题，然而该法需要决策者对故障模式进行两两对比并给出确定的数值，当产品或系统规模较大时，获取准确的关联信息变得非常困难；Emovon 等[7]分别采用 VIKOR 算法和基于妥协的均值算法来改进故障模式的排序方法，但对于信息的不确定性未能给出合适的表达方法；Mandal 等[8]使用相似度度量和可能性理论对 FMEA 信息的模糊表达方式进行改进；Rafie 等[9]提出一种模糊 FMEA 分析法，其中严重度 S 和难测度 D 根据模糊规则获取，而发生度 O 通过人工神经网络训练得到，因此应用该方法需要大量的样本；马存宝等[10]使用模糊理论来改进传统 FMEA 方法，在建立模糊评判模型后，使用基于 α 截集的解模糊方法来获取清晰化的评判矩阵，然后根据计算得到的 RPN 值进行排序，但由于该方法过早地应用解模糊技术，使得排序结果未能充分考虑初始数据包含的不确定信息；曹嘉容等[11]使用二元语义对 FMEA 分析系统的信息进行集结，并应用灰色理论计算关联度，进行故障模式排序。这些方法虽然能够在一定程度上弥补传统 FMEA 的缺陷，但实际应用的条件比较苛刻，计算也较复杂，特别是对于模糊语境下存在关联性的故障模式的风险排序问题还没有一个简便高效的方法。

鉴于此，本文提出一种基于有序加权平均算子（Ordered Weighted Averaging，OWA）和模糊 DEMATEL 法的混合方法，该方法不仅可以突破传统 RPN 方法的局限，还可以处理模糊语境下故障模式的相关性问题。其中，对故障模式的 3 个风险因子 O、S 和 D 用模糊语言来评价，对应评价值为三角模糊数的形式。由 OWA 算子得到的集结值表示故障模式间的直接影响度，然后通过模糊 DEMATEL 方法计算各故障模式的原因度，并按此进行风险排序。最后，以地铁车门系统的基础部件 FMEA 分析的应用实例来验证所提方法的可行性和有效性。

1 预备知识

1.1 OWA 算子

近年来，关于语言偏好信息方面的研究已有不少研究成果。其中，有序加权平均算子（OWA）是一种有效的集结数据信息的方法。OWA 算子基于权重向量的排序来获取向量属性的最优权重[12]。

定义 1 设 R^+ 为正实数集，$G_W: R^{+n} \to R^+$，令 $G_W(a_1, a_2, \cdots, a_n) = \sum_{j=1}^{n} w_j b_j$。其中，$W=(w_1, w_2, \cdots, w_n)^{\mathrm{T}}$ 为与 G 相关的指数加权向量，满足 $\sum_{j=1}^{n} w_j = 1$，且 $w_j \in [0,1]$。b_j 是一组数据 $(a_1, a_2, \cdots, a_n)$ 中第 j 大的元素。称函数 G 为有序加权平均算子，简称 OWA 算子。因此，OWA 算子是对 n 个数 $a_1, a_2, \cdots, a_n$ 按从大到小降序排列后进行的有序加权平均，且权重系数 w_j 与 a_j 无关，而与降序排在第 j 个位置的数 b_j 有关。若待处理数据为模糊数，则

$$\widetilde{G}_W(\widetilde{a}_1, \widetilde{a}_2, \cdots, \widetilde{a}_n) = \sum_{j=1}^{n} w_j \widetilde{b}_j \tag{1}$$

定义 2 设 OWA 集结算子中的权重向量为 $W=(w_1, w_2, \cdots, w_n)^{\mathrm{T}}$，则定义集结算子的 orness 测度为 $O(W) = \frac{1}{n-1} \sum_{j=1}^{n} (n-j) w_j$。并且 $O(W)=\alpha$，α 表示主观决策系数。α 的数值大小可以反映决策者的乐观度。比如，$\alpha=1$ 表示决策者保持纯乐观态度，此时 $W=(1,0,\cdots,0)$，最大属性值获得全部权重，OWA 算子变为最大化算子；$\alpha=0$ 表示决策者保持纯悲观态度，此时 $W=(0,0,\cdots,1)$，最小属性值获得全部权重，OWA 算子变为最小化算子；$\alpha=0.5$ 表示决策者保持中立态度，此时 $W=(\frac{1}{n}, \frac{1}{n}, \cdots, \frac{1}{n})$，所有属性值获得平均权重。

通过给定主观决策系数 α 和最大化信息熵可确定 OWA 权重向量。然后应用拉格朗日乘法规则将约束优化问题转化为多项式方程式，由此来确定能够实现最大信息熵的最优权重向量[13]，具体如下所示。

$$\ln w_j = \frac{j-1}{n-1} \ln w_n + \frac{n-j}{n-1} \ln w_1$$

由上式可得：

$$w_1 [(n-1)\alpha + 1 - n w_1]^n = ((n-1)\alpha)^{n-1} \cdot [((n-1)\alpha - n) w_1 + 1] \tag{2}$$

$$w_n = \frac{((n-1)\alpha - n) w_1 + 1}{(n-1)\alpha + 1 - n w_1} \tag{3}$$

$$w_j = \sqrt[n-1]{w_1^{n-j} w_n^{j-1}} \tag{4}$$

因此，通过式（2）可获得 w_1 的最优值，再根据式（3）确定 w_n，其余权重值可由式（4）确定。

1.2 模糊 DEMATEL

DEMATEL（Decision Making Trial and Evaluation Laboratory）即决策试行与评价实验方法，是用于分析复杂系统中各要素因果关系的一种方法。DEMATEL 以矩阵和有向图的形式揭示要素间的复杂关系。该方法在很多领域得到成功应用，比如知识管理、绩效分析、信息获取等。

现实中，由于人类语言固有的模糊性，使得决策者难以用准确的数字来量化要素间的影响强度。因此，本文将 DEMATAL 同模糊理论相结合来分析 FMEA 系统内要素的关联关系。模糊 DEMATEL 方法的步骤如下：

步骤 1 构建模糊初始直接影响矩阵。

$$\widetilde{\boldsymbol{Z}} = \begin{bmatrix} \widetilde{z}_{11} & \widetilde{z}_{12} & \cdots & \widetilde{z}_{1n} \\ \widetilde{z}_{21} & \widetilde{z}_{22} & \cdots & \widetilde{z}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \widetilde{z}_{n1} & \widetilde{z}_{n2} & \cdots & \widetilde{z}_{nn} \end{bmatrix}$$

其中，$\widetilde{z}_{ij} = (z_{ij1}, z_{ij2}, z_{ij3})$ 是三角模糊数，表示系统中要素 i 对要素 j 的影响强度。

步骤 2 建立规范化模糊直接影响矩阵。

$$\widetilde{X} = \frac{\widetilde{Z}}{r}, r = \max_{1 \leqslant i \leqslant n} (\sum_{j=1}^{n} z_{ij3}) \tag{5}$$

步骤 3 获取模糊综合影响矩阵。

令 $\widetilde{T} = (\widetilde{t}_{ij})_{n \times n}$，其代表综合影响矩阵，计算方法如下：

$$\widetilde{T}=\lim_{k\to\infty}(\widetilde{X}^1\oplus\widetilde{X}^2\oplus\cdots\oplus\widetilde{X}^k)=\widetilde{X}(\widetilde{I}-\widetilde{X})^{-1} \tag{6}$$

矩阵中的要素$\widetilde{t}_{ij}=(t_{ij1},t_{ij2},t_{ij3})$为三角模糊数形式，并且根据三角模糊数$\widetilde{t}_{ij}$将模糊综合影响矩阵$\widetilde{T}$中的要素划分为3个矩阵，分别为$T_1=[t_{ij1}]_{n\times n}=X_1(I-X_1)^{-1}$，$T_2=[t_{ij2}]_{n\times n}=X_2(I-X_2)^{-1}$，$T_3=[t_{ij3}]_{n\times n}=X_3(I-X_3)^{-1}$，而$I$是一个单位矩阵。对所有$i,j\in\{1,2,\cdots,n\}$，当$x_{ij1}<x_{ij2}<x_{ij3}$时，$T_1<T_2<T_3$。

步骤4　确定要素间的因果关联关系。

记$\widetilde{D}_i$和$\widetilde{R}_i$分别为矩阵$\widetilde{T}$中各行和各列元素的加和，其分别表示对应要素的影响度和被影响度。另记$\widetilde{P}_i=\widetilde{D}_i+\widetilde{R}_i$和$\widetilde{C}_i=\widetilde{D}_i-\widetilde{R}_i$分别代表对应要素的中心度和原因度。中心度代表要素在整个系统中的重要性，而原因度则代表要素在系统中的作用。当$C_i>0$时，说明该要素对系统中的其他要素的影响大，属于“原因型”要素；当$C_i<0$时，说明该要素受系统中其他要素的影响大，属于“结果型”要素。对于FMEA系统中的故障原因，其原因度越大，则风险越高。

2　混合FMEA模型

为了对评价信息进行有效地集结，本文利用OWA算子来处理风险评估信息，这样不仅解决了传统RPN方法中O、S、D等权重的问题，同时还考虑到了三者权重的动态分配。由此得到的OWA集结值作为模糊DEMATEL方法的输入，构建FMEA系统要素的初始直接影响矩阵，执行DEMATEL算法后最终输出系统要素的原因度，根据原因度对故障原因进行风险排序，据此找出需要改进的故障原因，提出相应的预防措施。

综合上述理论，基于模糊OWA算子和DEMATEL法的FMEA模型的流程图如图1所示。

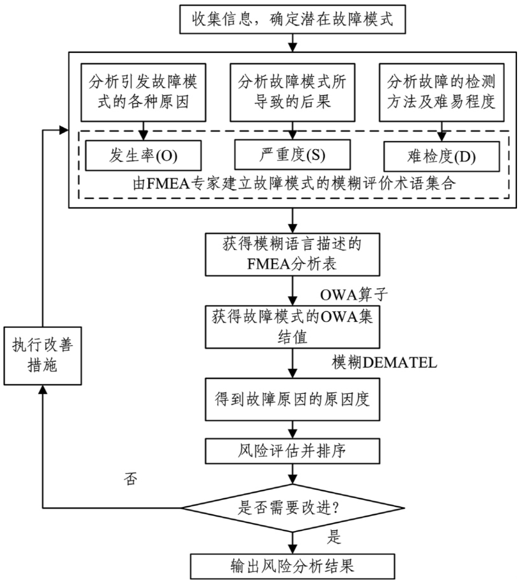


图1　混合FMEA模型流程图

具体步骤如下。

步骤1　列出潜在故障模式。FMEA专家根据历史数据和经验，列出产品或系统潜在的故障模式。

步骤2　列出所有引发故障模式的原因。FMEA专家研究判断产品或系统如何发生故障，以及会发生何种类型的故障模式，在FMEA表里列出引发故障模式的潜在故障原因。

步骤3　制定故障模式评估因子(包括发生率O、严重度S、难检度D)的模糊评价术语集合，如表1所列。专家对每一种故障模式的发生率、严重度、难检度进行模糊语言评价，评价信息根据表1转化为模糊三角数的形式。设有l个专家，若第k个专家关于某一故障模式的发生率给出的评价值为$\widetilde{c}^k$，则专家组的评价值为$\widetilde{c}=\sum_{k=1}^{l}\lambda_k\widetilde{c}^k$，其中$\lambda_k$表示第$k$个专家的权重。其他评估值的确定方法依此类推。

表1　传统评价术语对应的三角模糊值

语言评价术语		发生率O		严重度S		难测度D		模糊值
模糊语言	传统评估值	模糊语言	发生概率	模糊语言	传统评价	模糊语言	检出概率(%)	
极低(VL)	1	极少发生	<1∶20000	不影响使用	轻微	可轻易检出	86—100	(0,0,1)
低(L)	2,3	偶尔发生	1∶20000～1∶10000	影响外观	轻度	很大机会检出	66—85	(0,1,3)
中偏低(ML)	4	有时发生	1∶10000～1∶2000	有较小缺陷	略轻	较大机会检出	56—65	(1,3,5)
一般(M)	5,6	较常发生	1∶2000～1∶200	有较大缺陷	中等	有可能检出	46—55	(3,5,7)
中偏高(MH)	7	经常发生	1∶200～1∶20	有很大缺陷	略重	较小机会检出	36—45	(5,7,9)
高(H)	8,9	频繁发生	1∶20～1∶10	基本报废	严重	不大可能检出	16—35	(7,9,10)
极高(VH)	10	总是发生	>1∶10	危及安全	致命	几乎不能检出	0—15	(9,10,10)

步骤4　计算OWA权重。设定OWA算子的主观决策系数α，$\alpha\in[0,1]$。由式(2)—式(4)可得OWA权重。

步骤5　计算OWA集结值。根据步骤3和步骤4的信息由式(1)计算可得每种故障原因对应其故障模式的信息集结值。

步骤6　运用模糊DEMATEL方法进行FMEA分析。

1)构建FMEA系统的模糊初始影响矩阵，矩阵中的元素即为步骤5所得到的OWA集结值。

2)由式(5)得规范化模糊直接影响矩阵。

3)由式(6)得模糊综合影响矩阵。

4)分别计算故障模式和故障原因的中心度和原因度，明确因果关联。

步骤7　根据故障原因的原因度进行产品或系统的失效风险评估，并进行排序。

步骤8　对风险度大于设定阈值的故障模式执行改进措施，同时返回步骤3进行重新评估。

步骤9　当所有故障模式的风险度都小于设定阈值时，即可结束产品或系统的FMEA分析，并输出分析结果。

3　实例分析

为验证文中所提的基于OWA算子和模糊DEMATEL的风险评估方法的可行性和有效性，以某型号地铁车门系统的基础部件为分析对象，对其安全性进行FMEA分析，并将其与传统风险优先数法进行对比。该地铁车门系统基础部件的传统

FMEA 分析见表 2，其中 RPN 的值为发生频率 O、严重度 S 及难测度 D 3 个指标的评估值的乘积。

现有 FMEA 小组由 11 位专家组成，该专家组使用模糊语言对故障模式的 3 个风险因子进行评价，根据表 1 可得模糊语言对应的三角模糊值，对应评价信息如表 3 中第 4－6 列所示。该实例中，取主观决策系数 $\alpha=0.7$，则根据式(2)－式(4)可得 $\omega_1=0.554$，$\omega_2=0.292$，$\omega_3=0.154$。运用 OWA 法对评价信息进行集结，所得结果如表 3 中第 7 列所示。由 OWA 值可构建 FMEA 系统的初始影响矩阵(见图 2)，然后运用模糊 DEMATEL 法计算可得综合影响矩阵(见图 3)，据此计算各故障原因的原因度。对故障原因按照传统风险优先数 RPN 和模糊 OWA-DEMATEL 法的原因度进行排序，结果分别如表 2 和表 3 的最后一列所示。对比两种方法的排序结果可知：

(1)由传统 RPN 方法确定的风险最大的故障原因为 CF12，而本文方法所确定的风险最大的故障原因为 CF3。这是由于 CF3 会导致同时出现故障模式 FM1，FM3 和 FM4，因此虽然 CF12 的 RPN 比 CF3 的高，但实际上 CF3 的风险度更高。DEMATEL 方法分析系统是基于系统内各要素的相互影响关系的，充分考虑到了要素间的关联性，而传统 RPN 方法对系统要素的分析相对孤立，因此无法对内部存在关联性的系统作出准确的判断。

(2)由表 2 可知，CF1(3×8×2)和 CF10(2×6×4)的 RPN 值都为 48，而模糊 OWA-DEMATEL 法可将二者区分开来，其结果显示 CF1 较 CF10 风险度更高。这是由于后者在集结评价信息时对 3 个风险因子按排序给予不同的权重，而前者并未考虑 3 个风险因子的相对重要性，从而导致不同数值的风险因子组合，只要乘积相同则排序也一样。同理，对于 RPN 值相同的 CF13 和 CF15 以及 CF16 和 CF18，模糊 OWA-DEMATEL 法也能对其进行区分。因此，本文方法能够更准确地判断故障原因的相对风险，其精度更高。

表 2　地铁车门基础部件的潜在故障模式和故障原因分析表

序号	故障模式(FM)	故障原因(CF)	O	S	D	RPN	CF 风险排序
1	车门开关指示灯不亮(FM1)	开关指示灯损坏(CF1)	3	8	2	48	7
2	车门开关指示灯不亮(FM1)	锁闭行程开关损坏(CF2)	3	8	4	96	4
3	车门开关指示灯不亮(FM1)	门控器 EDCU 故障(CF3)	4	8	5	160	2
4	车门开关指示灯异常闪烁(FM2)	线路接触不良或存在异常(CF4)	2	5	3	30	14
5	车门切除指示灯常亮(FM3)	门控器 EDCU 故障(CF3)	4	5	5	100	2
6	车门切除指示灯常亮(FM3)	行程开关 S2 故障(CF5)	2	5	4	40	10
7	车门切除指示灯不亮(FM4)	门控器 EDCU 故障(CF3)	4	7	5	140	2
8	车门切除指示灯不亮(FM4)	切除指示灯损坏(CF6)	2	7	3	42	9
9	密封胶条松脱(FM5)	胶条未固定好(CF7)	4	7	4	112	3
10	密封胶条损坏(FM6)	胶条质量缺陷(CF8)	2	6	4	48	7
11	密封胶条损坏(FM6)	人为破坏(CF9)	2	6	3	36	11
12	未接接地线(FM7)	检修时漏接接地线(CF10)	3	4	2	24	15
13	接地线线鼻脱落(FM8)	线鼻未固定好(CF11)	3	6	2	36	11
14	嵌块磨损(FM9)	定位销与嵌块摩擦所致(CF12)	4	9	5	180	1
15	门页出现裂纹(FM10)	车门强度不够(CF13)	3	8	3	72	5
16	门页出现凹坑(FM11)	门页质量缺陷或乘客原因(CF14)	2	2	4	16	18
17	定位销与嵌块干涉(FM12)	移位，与嵌块或定位槽间隙过小(CF15)	3	6	4	72	5
18	定位销磨损(FM13)	定位销位置出现异常(CF16)	2	5	2	20	16
19	定位销断裂(FM14)	与定位槽磨损遭受较大应力(CF17)	3	4	3	36	11
20	缓冲头磨损(FM15)	长时间运用导致(CF18)	2	2	5	20	16

表 3　地铁车门基础部件安全性分析的模糊评估数据

序号	故障模式	故障原因	O	S	D	OWA 值	原因度	CF 风险排序
1	FM1	CF1	(0.9,2.8,4.8)	(5.1,7.1,9.1)	(0.6,2.2,4.2)	(3.181,5.090,7.090)	(0.138,0.221,0.308)	6
2	FM1	CF2	(1.5,3.5,5.5)	(5.1,7.1,9.1)	(2.2,4.2,6.2)	(3.699,5.699,7.699)	(0.161,0.248,0.335)	3
3	FM1	CF3	(1.7,3.7,5.7)	(5.1,7.1,9.1)	(3.3,5.3,7.3)	(4.051,6.051,8.051)	(0.479,0.739,1.000)	1
4	FM2	CF4	(0.4,1.7,3.7)	(3.3,5.3,7.3)	(0.7,2.3,4.3)1)	(2.094,3.870,5.870)	(0.088,0.168,0.255)	14
5	FM3	CF3	(1.7,3.7,5.7)	(3.0,5.0,7.0)	(3.3,5.3,7.3)	(2.966,4.966,6.966)	(0.479,0.739,1.000)	1
6	FM3	CF5	(0.4,1.7,3.7)	(3.0,5.0,7.0)	(1.6,3.6,5.6)	(2.191,4.083,6.083)	(0.095,0.177,0.264)	12
7	FM4	CF3	(1.7,3.7,5.7)	(5.0,7.0,9.0)	(3.3,5.3,7.3)	(3.995,5.995,7.995)	(0.479,0.739,1.000)	1
8	FM4	CF6	(0.8,2.5,4.5)	(5.0,7.0,9.0)	(0.8,2.5,4.5)	(3.127,4.993,6.993)	(0.135,0.217,0.304)	7
9	FM5	CF7	(1.6,3.6,5.6)	(5.1,7.1,9.1)	(1.6,3.6,5.6)	(3.539,5.539,7.539)	(0.154,0.241,0.328)	4
10	FM6	CF8	(0.6,2.2,4.2)	(4.0,6.0,8.0)	(1.7,3.7,5.7)	(2.805,4.743,6.743)	(0.120,0.206,0.293)	9
11	FM6	CF9	(0.5,2.3,4.3)	(4.0,6.0,8.0)	(1.0,3.0,5.0)	(2.585,4.554,6.554)	(0.112,0.198,0.285)	10
12	FM7	CF10	(1.0,3.0,5.0)	(1.8,3.8,5.8)	(0.3,1.5,3.5)	(1.335,3.212,5.212)	(0.058,0.140,0.226)	16
13	FM8	CF11	(1.0,3.0,5.0)	(3.4,5.4,7.4)	(1.0,3.0,5.0)	(2.222,4.114,6.114)	(0.097,0.179,0.266)	11
14	FM9	CF12	(1.5,3.5,5.5)	(6.7,8.7,9.7)	(3.4,5.4,7.4)	(4.936,6.936,8.382)	(0.214,0.301,0.364)	2
15	FM10	CF13	(1.0,3.0,5.0)	(4.4,6.4,8.4)	(2.2,4.2,6.2)	(3.234,5.234,7.234)	(0.141,0.227,0.314)	5
16	FM11	CF14	(0.8,2.5,4.5)	(0.3,1.5,3.5)	(1.5,3.5,5.5)	(0.631,2.100,4.100)	(0.027,0.091,0.178)	18
17	FM12	CF15	(1.4,3.4,5.4)	(4.0,6.0,8.0)	(1.5,3.5,5.5)	(2.870,4.870,6.870)	(0.125,0.212,0.299)	8
18	FM13	CF16	(0.5,2.1,4.1)	(3.0,5.0,7.0)	(0.6,2.1,4.1)	(1.914,3.707,5.707)	(0.083,0.161,0.248)	15
19	FM14	CF17	(0.8,2.5,4.5)	(2.8,4.8,6.8)	(1.2,3.2,5.2)	(2.025,3.979,5.979)	(0.091,0.173,0.260)	13
20	FM15	CF18	(0.4,1.7,3.7)	(0.3,1.6,3.6)	(3.0,5.0,7.0)	(1.104,2.608,4.608)	(0.048,0.113,0.200)	17

	CF1	CF2	⋯	CF17	CF18	FM1	FM2	⋯	FM14	FM15
CF1						(3.72,5.58,7.03)	0	0	0	0
CF2						(4.25,6.25,7.70)	0	0	0	0
⋮			0			⋮	⋮	⋮	⋮	⋮
CF17						0	0	0	(2.51,4.32,6.32)	0
CF18						0	0	0	0	(1.87,3.53,5.53)
FM1										
FM2										
⋮			0					0		
FM14										
FM15										

图 2　模糊初始直接影响矩阵

	CF1	CF2	⋯	CF17	CF18	FM1	FM2	⋯	FM14	FM15
CF1						(0.17,0.25,0.32)	0	0	0	0
CF2						(0.19,0.28,0.35)	0	0	0	0
⋮			0			⋮	⋮	⋮	⋮	⋮
CF17						0	0	00	(0.11,0.20,0.29)	0
CF18						0	0	0	0	(0.08,0.16,0.25)
FM1										
FM2										
⋮			0					0		
FM14										
FM15										

图 3　模糊综合影响矩阵

(3)由表 2 可知,CF9(2×6×3),CF11(3×6×2)以及CF17(3×4×3)这 3 个故障原因的 RPN 值相同,而模糊 OWA-DEMATEL 法能将此三者区分开来。一个原因如(2)中所述,是由于信息的有序加权集结。对比这 3 个故障原因的风险评价值,按照有序加权集合方法,严重度应该给予最大的权重,因此三者中 CF17 的排序最靠后。另一个原因则是评价信息的模糊处理。按传统的十分制评价标度,即使采用 OWA 方法对信息进行集结,仍将无法区分 CF9 和 CF11。而使用模糊语言来表达评估值,充分考虑了信息的不确定性,定性语言评价对应的评估数值是一个能够表达不确定性的模糊数,从而将原来具有相同 RPN 值的故障原因区分开来。

(4)从两个方法的排序结果来看,由于传统方法中 RPN 值重复率较高,因此很多故障原因排序一样,而本文方法得到的排序值(即原因度)没有重复,这为决策者制定预防失效措施提供了更明确的参考。

结束语　本文提出一种结合模糊 OWA 算子和模糊 DEMATEL 的方法来评价潜在故障模式的风险,该方法以更灵活的方式综合考虑故障模式的发生度、严重度和难测度。地铁车门系统基础部件的风险分析的应用实例证明了该方法的可行性和有效性,与传统 RPN 方法的对比表明该方法可以解决传统方法的固有缺点。特别是当故障模式的 RPN 值相同时,应用该方法可以很好地进行区分。另外,该方法可以为决策者提供更为准确、合理的故障风险排序,找出最关键的故障原因,以此为依据利用有限资源合理地安排改进或预防措施。

本文方法可以解决模糊语境下故障模式存在关联性的故障风险排序问题,其优势体现在以下几点:1)降低风险评估值的重复率;2)考虑故障模式的发生度、严重度和难测度的有序加权,即实现这 3 个风险因子权重的动态分配;3)该方法对于分析内部存在关联性的系统是非常有效的,是通过分析系统内部要素间的影响关系的强度来确定其排序;4)以模糊理论来表达 FMEA 中的故障信息,分析结果更贴近实际;5)为决策者提供了更有效、更精确的故障风险排序。

参 考 文 献

[1] Yang J, Huang H Z, He L P, et al. Risk Evaluation in Failure Mode and Effects Analysis of Aircraft Turbine Rotor Blades Using Dempster-Shafer Evidence Theory under Uncertainty [J]. Engineering Failure Analysis, 2011, 18(8): 2084-2092

[2] Vinodh S, Aravindraj S, Narayanan R S, et al. Fuzzy Assessment of FMEA for Rotary Switches: A Case Study [J]. The TQM Journal, 2012, 24(5): 461-475

[3] Kahraman C, Kaya L, Şenvar Ö. Healthcare Failure Mode and Effects Analysis under Fuzziness [J]. Human and Ecological Risk Assessment, 2013, 19(2): 538-552

[4] Liu H C, Liu L, Lin Q L. Fuzzy Failure Mode and Effects Analysis Using Fuzzy Evidential Reasoning and Belief Rule-Based Methodology [J]. IEEE Transactions on Reliability, 2013, 62(1): 23-36

[5] Zhou Q, Thai V V. Fuzzy and grey theories in failure mode and effect analysis for tanker equipment failure prediction[J]. Safety Science, 2016(83): 74-79

[6] Lolli F, Ishizaka A, Gamberini R, et al. FlowSort-GDSS-A novel group multi-criteria decision support system for sorting problems with application to FMEA[J]. Expert Systems with Applications, 2015, 42(17): 6342-6349

[7] Emovon I, Norman R A, Alan J M, et al. An integrated multicriteria decision making methodology using compromise solution methods for prioritising risk of marine machinery systems[J]. Ocean Engineering, 2015, 105(10): 92-103

[8] Mandal S, Maiti J. Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach[J]. Expert Systems with Applications, 2014, 41(7): 3527-3537

[9] Rafie M, Namin F S. Prediction of subsidence risk by FMEA using artificial neural network and fuzzy inference system[J]. International Journal of Mining Science & Technology, 2015, 25(4): 655-663

[10] 马存宝,李雯,孙焱,等.基于模糊理论的 FMEA 方法研究[J].

测控技术,2013,32(8):137-140

[11] 曹嘉容,王瑛,支乐. 基于二元语义与灰色关联决策的改进 FMEA 方法[J]. 空军工程大学学报(自然科学版),2014(5):92-95

[12] Chang K H,Chang Y C,Wen T C,et al. An innovative approach integrating 2-tuple and LOWGA operators in process failure mode and effects analysis [J]. International Journal of Innovative Computer Information & Control,2012,8(1):747-761

[13] Fuller R,Majlender P. An analytic approach for obtaining maximal entropy OWA op erator weights [J]. Fuzzy Sets & Systems,2001,124(124):53-57

(上接第 345 页)

进行打分,该打分是经过 XX 公司多年的应用总结出的特别精确的判定分数,如表 5 所列。

表 5 阈值检测 16 项标准打分值

sp_id	sp_score	sp_expr
26112	30	文件名有数字前缀
26113	30	文件使用系统图标
26114	60	API 数量异常
26115	20	文件在系统路径下
26116	30	文件无版权信息
26117	10	文件长度过大
26118	60	文件有多扩展名
26119	10	有非正常节名
26120	70	处于启动项中
26121	30	文件最近创建
26122	50	仿造系统文件名
26123	30	文件使用加壳
26124	50	文件监听端口
26125	40	文件包含恶意 API
26126	20	文件中包含邮件信息
26127	50	嵌入 PE 程序
36866	150	阈值

该方法应用时主要面向实际系统中需要高响应速度、高准确率的恶意代码分析。分析时的样本数据集用于特征向量空间构建,主要包含白样本和黑样本,其中,白样本集主要从 Windows 系统提取相关文件,黑样本集主要通过反病毒厂商样本交换及网络蜜罐捕获积累的样本,用作快速恶意代码分析的参考空间和佐证。

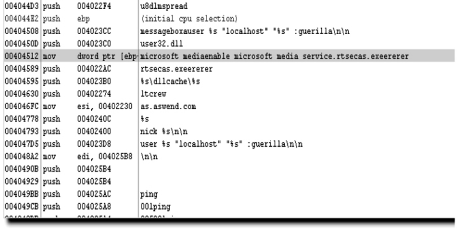
实际 Backdoor. Win32. IRCBot. bad 恶意代码快速分析过程如下。

(1)恶意代码环境

病毒名称为 Backdoor. Win32. IRCBot. bad,病毒类型为后门类,文件 MD5 为 87A7C70B7295C5CE90E171447243E875,公开范围为完全公开,危害等级为 3,文件长度为 43520 字节,感染系统为 Windows98 以上版本,开发工具为 Microsoft Visual C++,加壳类型为 PECompact V2. X-> Bitsum Technologies。

(2)静态分析

观察文件,该文件为一个 43kB 的 exe 文件。该文件没有版本信息,文件属性为系统隐藏,文件路径为系统备份文件目录。文件创建进程、开启服务、打开端口、连接网络。初步分析为一个后门程序。用 autoruns 查看其创建的服务。



Address	Disassembly		Text String
00404497	push	004023A4	192.168.0.2%s\dllcache\%s
0040449C	push	00402230	as.aswend.com
004044A6	push	0040239C	#erer
004044AB	push	00402244	#eeeeee#eeeeee#eeeeee#eeeee
004044BF	push	00402384	:*!*@contr0lling.b0tnet#erer
004044C4	push	00402264	:*!*@h4ckers
004044CE	push	0040237C	pwn3d
004044D3	push	004022F4	u8dlmspread
004044E2	push	ebp	(initial cpu selection)
00404508	push	004023CC	messageboxauser %s "localhost" "%s" :guerilla\n\n
0040450D	push	004023C0	user32.dll
00404512	mov	dword ptr [ebp	microsoft mediaenable microsoft media service.rtsecas.exeererer
00404589	push	004022AC	rtsecas.exeererer
00404595	push	004023B0	%s\dllcache\%s
00404630	push	00402274	ltcrew
004046FC	mov	esi, 00402230	as.aswend.com
00404778	push	0040240C	%s
00404793	push	00402400	nick %s\n\n
004047D5	push	004023D8	user %s "localhost" "%s" :guerilla\n\n
004048A2	mov	edi, 004025B8	\n\n
0040490B	push	004025B4	
00404929	push	004025B4	
004049BB	push	004025AC	ping
004049CB	push	004025A8	001ping

图 2 恶意代码静态分析

从恶意代码程序的字符串中可以看到恶意代码释放文件的路径,创建服务名称及其描述,如图 2 所示。

(3)动态分析

////病毒运行后把自身拷贝为%System%\dllcache\Rtsecas. exe,删除自身,设置文件属性为系统、隐藏、只读。

0040460B 8D85 E4FEFFFF LEA EAX,DWORD PTR SS:[EBP-11C]

00404611 6A 07 PUSH 7;参数:隐藏、系统、只读

00404613 50 PUSH EAX

00404614 FF15 60204000 CALL DWORD PTR DS:[〈&kernel32. S〉;调用 SetFileAttributesA 设置文件属性为系统、隐藏、只读。

该病毒为后门类,病毒运行后把自身拷贝为%System%\dllcache\Rtsecas. exe,并删除自身;创建名为 Microsoft Media 的服务,链接 IRC 服务器接受控制,创建线程扫描本地网络,并对其进行攻击。

4.2 恶意代码处置

先对恶意代码进行非感染式恶意代码手动处置,然后再对感染的正常文件进行程序清除,但很容易在手动处置的同时运行已被感染的正常文件。因此针对感染式恶意代码一般不进行手动处置,而是直接根据感染式恶意代码的分析,编写程序进行程序处置。

程序的编写除了进行非感染式恶意代码程序处置部分,还要编写清除模块。清除模块包括两个最主要的部分:感染式特征匹配和针对此恶意代码编写修复模块。

结束语 本技术的工作流程与实现技术面向恶意代码分析的实际需求,研究了进行现场快速分析和处置恶意代码的方法,构建了环境分析、文件细化、静态分析、动态分析恶意代码快速分析处置的具体模型,结合快速阈值检测理论,达到了基于快速阈值分析适合现场恶意代码快速分析的和处置的目的。在此基础上,实现了对笔者所在单位遇到的恶意代码的实例分析。

参 考 文 献

[1] Branco R R,Shamir U. Architecture for automation of malware analysis[C]// The 5th International Conference on Malicious and Un-wanted Software (MALWARE). 2010:106-112

[2] Egele M,Scholte T,Kirda E,et al. A survey on automated dynamic malware-analysis techniques and tools[J]. ACM Computing Surveys (CSUR),2012,44(2):1-42

[3] Sathyanarayan V S,Kohli P,Bruhadeshwar B. Signature generation and detection of malware families[C]// Information Security and Privacy. 2008:336-349

[4] Staish S,Pereira S. Behavioral Signature Generation Using Clustering:WIPO Patent 2011137083[P]. 2011

[5] http://www. m86security. com/newsimages/trace/Marshal8e6_TRACE_Report_July_2015. pdf