一种基于信息熵的体系流程脆弱性分析方法

韦正现[1,2],宋敏[3*],童鹏鹏[4],王红滨[4]

1. 国防科技工业海洋安全体系创新中心,北京 100036
2. 青岛海洋科学与技术试点国家实验室,青岛 2660011
3. 北京外国语大学信息技术中心,北京 100089
4. 哈尔滨工程大学计算机科学与技术学院,哈尔滨 150001

摘要 体系在执行任务过程中面临来自外部、内部的各种破坏、干扰或威胁等风险,当风险发生时体系受到影响的程度表现为体系脆弱性,体系流程的脆弱性是影响体系能否完成任务的一个重要方面。提出一种基于信息熵的体系流程脆弱性分析方法:首先,面向体系面临的风险事件及其流程结构特征建立体系流程结构脆弱性分析过程;其次,将体系流程转化为有向图模型,基于信息熵构建了体系流程中各个节点的脆弱度计算模型;最后,将复杂体系流程有向图模型简化为串联、并联和混合3种基本结构,建立了3种基本结构的脆弱度计算模型,进而即可计算体系流程的脆弱度。通过案例说明了该方法的有效性。

关键词 信息熵;体系流程;脆弱性分析

"体系"(system-of-systems,SoS)的概念已经出现很长时间[1],许多不同领域的学者和组织也从他们各自的领域背景和角度提出了体系的定义,然而目前没有一个被普遍接受的定义。体系是系统的联接,在系统联接的体系中允许系统间进行相互协同与协作,如信息化战场的C^4I(command, control, computers, communications, information)与ISR(intelligence, surveillance reconnaissance)系统[2]。体系是系统的综合,系统综合以系统的演化发展、协同与优化为目的,最终达到提高整体效能的宗旨[3]。体系是相互协作的系统的集成,这些组成系统具备两种附加特性,即运作的自主性与管理的自主性[4-5]。美国国防部指出"互相依赖的系统组合链接,提供的能力远大于这些系统的能力之和"[6]。从上这些体系定义上看,体系由分布在不同位置的成员系统通过网络链接起来形成复杂的有机整体。从网络结构上看,各个成员构成了网络中各个节点。

体系在执行任务过程中将面临来自外部和内部的各种风险、干扰或威胁,给任务的完成造成影响。例如海上编队体系在实施作战过程中,装备成员不仅面临着电磁压制、攻击和干扰的软对抗威胁,而且面临受到导弹、炮弹、鱼雷等的硬杀伤威胁,或者体系内部可能存在的可靠性、安全性等事件,导致武器装备体系网络链接中断或者成员故障、损伤等退出体系的风险,导致体系整体作战能力和效能受到极大影响。当体系发生

收稿日期:2019-01-22;修回日期:2019-05-15

基金项目:国家自然科学基金项目(61502037,16772152);国防科技创新特区项目(18-H863-05-ZT-001-007-02)

作者简介:韦正现,研究员,研究方向系统工程、体系工程和人工智能等,电子信箱:weizhengxian@sina.com;宋敏(通信作者),工程师,研究方向为软件可靠性、数据库和软件体系结构,电子信箱:songmin@bfsu.edu.cn

引用格式:韦正现, 宋敏, 童鹏鹏, 等. 一种基于信息熵的体系流程脆弱性分析方法[J]. 科技导报, 2019, 37(13): 40-46; doi: 10.3981/j.issn.1000-7857.2019.13.005

各种风险、干扰或威胁(统称为风险事件,如攻击、破坏或故障等)时体系受到的影响程度,称为体系的脆弱度。在体系执行任务的过程中,从体系面临的风险事件入手,对体系流程的脆弱性进行分析,找出流程中的脆弱点,并计算出流程整体的脆弱度,以便有效采取各种预案与应对措施,确保体系具有极强的健壮性与生命力。由于体系在执行任务的过程中,不仅面临十分复杂的外部环境因素的影响,而且面临体系内部网络中断、节点故障和成员退出等风险事件,导致体系流程脆弱性分析具有明显的模糊性和不确定性。为此,提出一种基于信息熵的体系流程脆弱性分析方法。

1　体系流程结构脆弱性分析过程模型

目前脆弱性在不同的领域有不同含义[7-9]。体系在执行任务过程中将面临来自外部环境的各种破坏、干扰或威胁等风险因素,同时在内部存在体系成员的故障、失效或网络中断等潜在隐患因素,当这些情况发生时(即形成风险事件),会作用于体系,可能会导致体系执行任务效果降低,甚至致使任务中断,此时体系表现出它的脆弱性。为了使体系具有极强的健壮性与生命力,需要在分析度量体系脆弱性的基础上,根据影响因素的作用方式,采取相应的预案和措施等对策,并实施于体系开发或使用阶段,以便满足体系完成任务的需求。体系脆弱性分析的因素关系如图1所示。

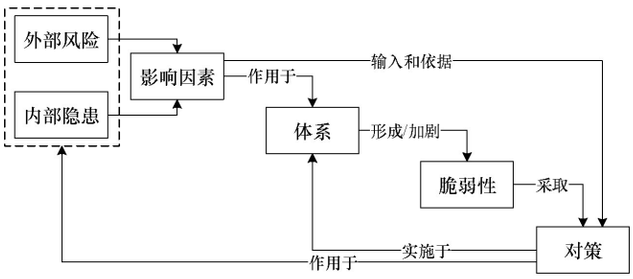

图1　体系的脆弱性因素关系

Fig. 1　Factors relationship of SoS vulnerability

体系通过其流程的实施来完成任务,因此需要分析体系流程的脆弱度界定相关影响因素和风险事件对体系完成任务的影响程度。流程将各个节点组织成为有机的整体,从网络结构上看,体系流程是由多个成员节点连接构成的复杂有向图(directed graph),根据有向图的性质,体系流程的脆弱度不仅受到流程中各节点脆弱度的影响,同时也与体系流程结构相关。因此,在度量评价体系流程的脆弱度时需要从节点的脆弱度和流程结构的脆弱度两个方面进行综合分析。体系流程脆弱度的分析过程如图2所示。

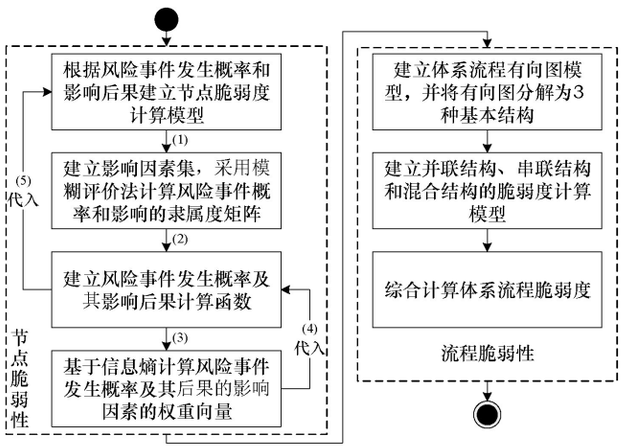

图2　体系流程脆弱度分析过程模型

Fig. 2　SoS flow vulnerability analysis process model

图2中,对于节点脆弱度的分析,首先根据风险事件发生概率和风险事件发生后产生的影响后果,建立节点脆弱度计算模型;计算过程中需要确定风险事件发生概率及其后果的影响因素集,由于这些影响因素对于风险事件发生及其后果的影响作用具有模糊性和不确定性,利用模糊评价法建立影响因素对风险概率及其后果的隶属度矩阵;然后,建立具体的风险事件发生概率和风险事件产生影响后果的计算函数;针对计算函数中需要确定各个影响因素指标的权重向量,采用信息熵进行求解[10-11],并代入计算函数中;最后综合计算出节点的脆弱度。对于体系流程脆弱度的分析,以节点脆弱度为基础,建立体系流程有向图模型,并将有向图分解为串联、并联和混合3种基本结构,建立串联结构、并联结构和混合结构的脆弱度计算模型,然后根据实际的体系流程综合计算出其脆弱度。

2　基于信息熵的节点脆弱度计算模型

体系流程由各节点组成,为了分析体系流程的脆弱度,需要先分析节点的脆弱度。节点的脆弱度是由作用于该节点的风险事件所引发。风险事件对节点脆弱性的影响从两个方面进行分析,一方面是风险事件发生概率,另一方面是风险事件发生后所产生影响后

果。P_f和P_s分别表示风险事件未发生与风险事件发生的概率。C_f和C_s的分别表示风险事件未发生和发生的影响函数,其域值为区间[0,1]。显然有

$$P_f=1-P_s \tag{1}$$

$$C_f=1-C_s \tag{2}$$

节点的脆弱度V_{node}是风险事件(P)、风险事件影响后果(C)的似然估计,如下:

$$\begin{aligned} V_{node}&=f(P,C)\\ &=1-P_fC_f\\ &=1-(1-P_s)(1-C_s)\\ &=P_s+C_s-P_sC_s \end{aligned} \tag{3}$$

从式(3)可以看出,只要求出节点风险事件发生的概率P_s和风险事件发生后产生的影响C_s,就可以得到节点脆弱度。

体系面临来自外部环境的各种破坏、干扰或威胁等风险因素,同时在内部存在体系成员的故障、失效或网络中断等的潜在隐含因素,风险事件发生概率和风险影响的估计具有一定的模糊性和不确定性。这里采用模糊评价法[11-12]进行分析。节点风险分析具体步骤如下。

2.1 建立隶属度矩阵R

对于节点的风险事件发生概率和风险事件发生后所产生影响,构造影响因素集,设为$U=\{U_1, U_2, \cdots, U_n\}$。然后构造评判集,设为$V=\{V_1,V_2,\cdots, V_n\}$,对于体系中节点的风险事件发生概率和风险事件产生的影响,根据它们特性可以设立不同的评判集。

评价者参照评判集V对影响因素集U中的各影响因素进行评价,根据各个不同影响因素特征给出相应的评语,构造模糊映射$f: V\rightarrow F(V)$,$F(V)$是V上的模糊全集,则有$U_i\rightarrow f(U_i)=(r_{i1}, r_{i2}, \cdots, r_{im})$,映射$f$表示影响因素$U_i$对评判集中各评语的支持程度。令影响因素$U_i$对评判集$V$的隶属向量为$\boldsymbol{R}_i=\{r_{i1}, r_{i2}, \cdots, r_{im}\}$, i=1, 2, …, n,有

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m}\\ r_{21} & r_{22} & \cdots & r_{2m}\\ \vdots & \vdots & \vdots & \vdots\\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix} \tag{4}$$

于是得到U关于V的隶属度矩阵$\boldsymbol{R}$。对于节点脆弱性分析来说,影响因素对于风险事件发生概率和风险事件发生后所产生影响的隶属度矩阵,分别设为$\boldsymbol{R}_p$和$\boldsymbol{R}_c$。

2.2 P_s和C_s的计算

在体系中,计算各个节点的风险事件发生概率时,设各个影响因素的权重向量为

$$\boldsymbol{A}_p=(a_{p1},a_{p2},\cdots,a_{pn}) \tag{5}$$

同样对于评判集V,为各评判集成员(指标)赋予相应的权重,得到权重向量

$$\boldsymbol{B}_p=(b_{p1},b_{p2},\cdots,b_{pm}) \tag{6}$$

则风险事件发生的概率为

$$P_s=\boldsymbol{A}_p\boldsymbol{R}_p\boldsymbol{B}_p^T \tag{7}$$

同样,在计算体系各节点风险事件产生后的影响时,设各影响因素相应的权重向量

$$\boldsymbol{A}_c=(a_{c1},a_{c2},\cdots,a_{cn}) \tag{8}$$

对评判集V,为各指标赋予相应的权重,得到权重向量

$$\boldsymbol{B}_c=(b_{c1},b_{c2},\cdots,b_{cm}) \tag{9}$$

则风险事件产生后的影响为

$$C_s=\boldsymbol{A}_c\boldsymbol{R}_c\boldsymbol{B}_c^T \tag{10}$$

在计算P_s和C_s的中,需要确定两个部分的权重向量,分别为$\boldsymbol{A}_p$和$\boldsymbol{A}_c$。根据信息熵理论,由各节点影响因素传递给评价者信息量的大小来确定相应影响因素的权重,反映不同影响因素在评价中所起作用的大小,影响因素所提供的信息量越多,则该影响因素在评价中所起的作用就越大,由信息熵确定的权重就越大;反之,影响因素所提供的有用信息较少,由信息熵确定的权重就越小,说明该因素就越不重要。影响因素信息量的多少和质量的高低决定着评价的精度。由此这里采用信息熵计算$\boldsymbol{A}_p$和$\boldsymbol{A}_c$。

2.3 基于信息熵计算A_p和A_c

对构造的影响因素集U,如果某因素U_i,对于评判集中各指标的支持度$\boldsymbol{r}_{ij}$差距越大,则该因素在综合评价中所起的作用越大;如果某因素的各指标支持度全部相等,即评定结果太分散,凝聚力差,则对该因素的评定在综合评价中几乎不起作用。信息熵$H=-\sum_{i=1}^{n}P_iL_nP_i$表示信息的有序程度。由熵的极值性可知$P_i$越接近相等,熵值越大。影响因素对节点脆弱度评估的不确定性就越大。因此,可根据各影响因素对评判集中各指标的支持度r_{ij},利用信息熵,计算各因素的权重向量。

影响因素U_i的相对重要性可由熵来度量

$$H_i=-\sum_{j=1}^{m}r_{ij}L_nr_{ij} \tag{11}$$

式中,r_{ij}(j=1, 2, …, m)越接近相等,熵值越大,影响因素U_i对节点脆弱度评估的不确定越大。当r_{ij}(j=1, 2, …,

m)取值相等时,熵最大:$H_{max}=L_n m$,用H_{max}对式(11)进行归一化处理,就得到衡量影响因素U_i的相对重要性的熵值

$$e_i=-\frac{1}{L_n m}\sum_{j=1}^{m} r_{ij}\lg r_{ij} \tag{12}$$

式中,$0\leqslant e_i\leqslant 1$。当$r_{ij}$($j$=1, 2, …, m)取值相等时,e_i=1,此时熵最大。当熵最大时,此影响因素对节点脆弱度评估的贡献最小,所以确定影响因素U_i的权值可以由$1-e_i$来度量。

对其进行归一化得到影响因素U_i的权值ϕ_i为

$$\phi_i=\frac{1}{n-E}(1-e_i) \tag{13}$$

式中,$E=\sum_{i=1}^{n} e_i$;ϕ_i满足:$0\leqslant\phi_i\leqslant 1$,$\sum_{i=1}^{n}\phi_i=1$。

如果评价者对各影响因素凭借经验有主观的判定权值,设为W_i,则可以将主观判定和客观判定相结合,得到综合权值

$$\sigma_i=\frac{\phi_i W_i}{\sum_{i=1}^{n}\phi_i W_i} \tag{14}$$

如果没有主观判定,则可以由ϕ_i直接作为各因素权重。

在体系流程的节点脆弱度计算过程中,根据式(4)计算$\boldsymbol{R}_p$和$\boldsymbol{R}_c$,通过式(13)、式(14)计算出$\boldsymbol{A}_p$和$\boldsymbol{A}_c$后,然后将$\boldsymbol{R}_p$、$\boldsymbol{R}_c$、$\boldsymbol{A}_p$和$\boldsymbol{A}_c$代入式(7)、式(9),就可以计算出P_s和C_s,最后通过式(3)可以计算出节点的脆弱度。在计算各个节点的脆弱度之后,以此为基础,可以进一步分析体系流程的脆弱度。

3　体系流程结构脆弱性分析模型

体系中大多数节点一般都分布在不同物理位置,具有行为的自主性、管理的独立性等,通过网络实现信息共享和行为交互,形成能够完成特定任务的流程。体系流程的脆弱性是影响体系能否完成任务的一个重要方面。体系流程结构很复杂,为确保体系具有很强的健壮性和可用性,很多节点采用了冗余容错设计。为了简化体系流程脆弱性的分析,将复杂的流程有向图简化为串联、并联和混合3种基本结构,通过计算这3种基本结构的脆弱度,再进行综合计算出体系流程的脆弱度。

3.1　串联结构

流程中的每个节点都没有设置冗余容错节点。如图3所示,流程从a节点开始执行到d节点,来完成一个任务(或子任务)。在该流程结构进行脆弱度计算时,使用串联结构的计算方法。

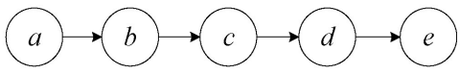

图3　串联结构

Fig. 3　Series structure

通过式(15)能够求出流程的脆弱度

$$V_{path}=1-\prod_{i=0}^{n}(1-V_i) \tag{15}$$

式中,V_i为第i个节点的脆弱度;n为流程的节点数。

当该流程的脆弱度低于预设值时,需要对该流程中脆弱度低的节点进行分析,以便采取有效预防措施。

3.2　并联结构

在体系中,一些关键路径如无法成功执行会导致非常严重的后果,为了确保这些关键路径在复杂的外部环境行下能够顺利执行,通常采用冗余容错设计,如图4所示。这3条路径具有相同的功能,任何一条路径能够正常执行都可以确保体系整体获得正确的结果。

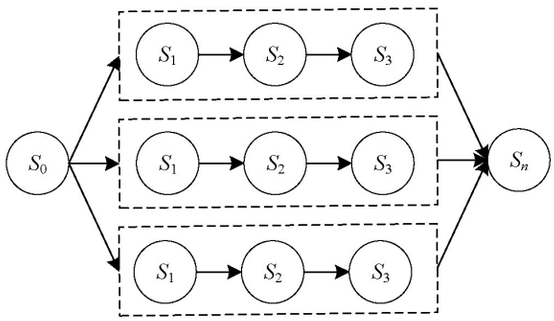

图4　并联结构

Fig. 4　Parallel structure

如图4所示并联结构,使用式(16)对其脆弱度进行计算

$$V_{path}=\prod_{j=0}^{m}\left[1-\prod_{i=0}^{n}(1-V_i)\right] \tag{16}$$

式中,n表示路径中节点的个数;m代表冗余的流程路径数。

3.3　混合结构

混合结构是并行结构和串行结构混合在一起,如图5所示。在图5中,节点b和d是容错节点,该流程执

行过程中b和d的其中一个节点正常工作,就能确保该流程不会因为b和d中一个节点故障、失效而导致无法执行。

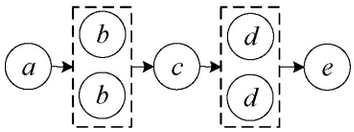

图5 混合结构

Fig. 5 Combination structure

对混合结构的脆弱度计算公式如下:

$$V_{\text{path}}=1-\prod_{i=0}^{n}\left(1-\prod_{k=0}^{l}V_k\right) \tag{17}$$

式中,V表示该流程结构执行路径的脆弱度;n表示该路径所使用的节点数;l表示处于i位置容错的节点数量,当n=1时表示该节点没有设置容错节点,只有1个节点;V_i表示节点i的脆弱度。

复杂体系流程通过上述3种基本流程结构组合后形成,就可以通过采用3种基本结构的脆弱度,进而计算体系流程的脆弱度。

4 案例分析

体系流程的脆弱性需要从节点本身面临的风险事件及流程结构特性进行综合分析。本节通过简化的体系反导流程为例说明体系流程脆弱性分析方法的有效性。假设某体系反导的流程如图6所示。

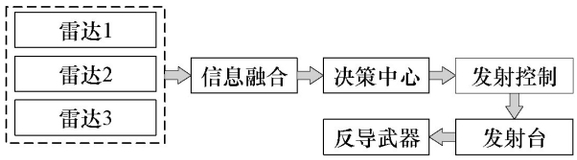

图6 体系流程案例

Fig. 6 Case of SoS flow

首先以其中一个雷达节点1为例子,计算该节点的脆弱度,详细过程如下。

1)假设雷达节点存在6个影响因素,构造集合U={$U_1,U_2,\cdots,U_6$},其中$U_1,U_2,\cdots,U_6$分别表示“节点受到攻击”“操作失误”“响应时间长”“软件错误”“网络链接中断”和“硬件故障”。

2)在构造评判集,对于风险事件概率发生,影响因素U的评判集V={$V_1,V_2,\cdots,V_7$},分别代表的概率等级“可忽略”“很低”“低”“中等”“高”“很高”“极高”。由评价者参照评判集对影响因素U进行概率评价,每个评判者对各个影响因素的确定其风险概率为$V_1,V_2,\cdots,V_7$中的一种。

3)结合各个评价者的评定意见,计算出各影响因素隶属于各个指标的概率,则可得隶属度矩阵

$$\boldsymbol{R}_{\text{p}}=\begin{bmatrix}0.25&0&0.5&0.25&0&0&0\\0&0.25&0.75&0&0&0&0\\0.5&0.5&0&0&0&0&0\\0&0.5&0&0.5&0&0&0\\0&0.5&0.25&0.25&0&0&0\\0&0.75&0&0.25&0&0&0\end{bmatrix}$$

4)各个影响因素的权重向量首先使用式(12)计算e_i,然后利用e_i求出$\boldsymbol{A}_{\text{p}}$。

5)求评判集各指标向量$\boldsymbol{B}_{\text{p}}$。确定评判集中各标准确定评判集中各标准$V_1,V_2,\cdots,V_7$的权重依次为1/28、2/28、3/28、4/28、5/28、6/28、7/28,即指标向量$\boldsymbol{B}_{\text{p}}$=(1/28、2/28、3/28、4/28、5/28、6/28、7/28)。

6)按照式(7),$P_{\text{s}}=\boldsymbol{A}_{\text{p}}\boldsymbol{R}_{\text{p}}\boldsymbol{B}_{\text{p}}^{\text{T}}$,计算出风险事件发生的概率为

$$\boldsymbol{P}_{\text{s}}=\boldsymbol{A}_{\text{p}}\begin{bmatrix}0.25&0&0.5&0.25&0&0&0\\0&0.25&0.75&0&0&0&0\\0.5&0.5&0&0&0&0&0\\0&0.5&0&0.5&0&0&0\\0&0.5&0.25&0.25&0&0&0\\0&0.75&0&0.25&0&0&0\end{bmatrix}\begin{bmatrix}1/28\\2/28\\3/28\\4/28\\5/28\\6/28\\7/28\end{bmatrix}$$

7)对于风险事件的影响来说,影响因素集U的评判集$V=\{V_1,V_2,\cdots,V_5\}$,其定义为“可忽略的”“微小”“一般”“较严重”“严重”。对影响因素U进行影响评定,则得到隶属度矩阵$\boldsymbol{R}_{\text{c}}$

$$\boldsymbol{R}_{\text{c}}=\begin{bmatrix}0.25&0&0.75&0&0\\0&0.25&0.5&0.25&0\\0.25&0&0&0.75&0\\0&0.25&0&0.75&0\\0&0&0&0.25&0.75\\0&0&0&0.25&0.75\end{bmatrix}$$

8)各影响因素的权重向量首先使用式(12)计算e_i,然后利用e_i求出$\boldsymbol{A}_{\text{c}}$。

9)对于评判集各指标向量$\boldsymbol{B}_{\text{c}}$。确定评判集中各标

准 V_1, V_2, …, V_5的权重依次为1/25,3/25,5/25,7/25,9/25,即指标向量$\boldsymbol{B}_c$=(1/25,3/25,5/25,7/25,9/25)。

10) 按照式(10),计算出风险事件的影响后果为

$$\boldsymbol{C}_s=\boldsymbol{A}_c\begin{bmatrix}0.25 & 0 & 0.75 & 0 & 0\\ 0 & 0.25 & 0.5 & 0.25 & 0\\ 0.25 & 0 & 0 & 0.75 & 0\\ 0 & 0.25 & 0 & 0.75 & 0\\ 0 & 0 & 0 & 0.25 & 0.75\\ 0 & 0 & 0 & 0.25 & 0.75\end{bmatrix}\begin{bmatrix}1/25\\ 3/25\\ 5/25\\ 7/25\\ 9/25\end{bmatrix}$$

11) 通过式(3)得$V_{node}=P_s+C_s-P_sC_s$=0.67163,该值即为雷达节点1的脆弱度。

12) 按照上述过程可以计算出其他节点的脆弱度。在图6假设3个雷达节点的脆弱度相同,且其中有一个能够工作,流程就可以继续执行,其他节点出现故障,则整个该流程将无法完成,根据式(17)该体系流程案例的脆弱度为V_{path}=0.70061。

从上述分析结果看,雷达节点的脆弱度和该流程的脆弱度都很高,表明一旦在该流程中风险事件发生,则对该流程所执行的任务将会产生很大的影响,需要采取相应的预案或措施(例如热备份或冷备份等),来降低该流程的脆弱度,使其更具有健壮性与生命力。

5　结论

体系在执行任务过程中面临来自外部、内部的各种破坏、干扰或威胁等风险,当风险发生时体系受到影响的程度表现为体系脆弱性,体系流程的脆弱性是影响体系能否完成任务的一个重要方面。通过对体系脆弱性进行分析,可以确定复杂体系流程中脆弱的节点与流程路径,以便有效采取各种预案与应对措施,确保体系具有极强的健壮性与生命力。为了能够对体系流程的脆弱性进行量化分析,面向体系面临的风险事件及其流程结构特征建立体系流程结构脆弱性分析过程,将体系流程转化为有向图模型,利用模糊评价法建立影响因素对风险概率及其后果的隶属度矩阵,基于信息熵构建了体系流程中各个节点的脆弱度计算模型,同时将复杂体系流程有向图模型简化为串联、并联和混合3种基本结构,建立了3种基本结构的脆弱度计算模型,通过3种基本结构脆弱度计算模型的组合就可以计算体系流程的脆弱度。通过计算体系流程的脆弱度,为体系流程设计提供指导,同时可以在体系执行过程中根据流程的脆弱度变化情况,提前采取相应策略与措施,确保体系具有较高的任务执行能力。

参考文献(References)

[1] Lane J A, Valerdi R. Synthesizing SoS concepts for use in cost modeling[J]. Systems Engineering, 2007, 10(4): 297-308.

[2] Manthorpe Jr W H. The emerging joint system of systems: A systems engineering challenge and opportunity for APL[J]. John Hopkins APL Technical Digest, 1996, 17(3): 305-313.

[3] Pei R S. Systems-of-systems integration (SoSI)—A smart way of acquiring army C4I2WS systems[C]// Proceedings of the Summer Computer Simulation Conference. New York: ACM, 2000: 574-579.

[4] Sage A P, Cuppan C D. On the systems engineering and management of systems-of-systems and federations of systems[J]. Information, Knowledge, Systems Management, 2001, 2(4): 325-345.

[5] Maier M W. Architecting principles for systems-of-systems[J]. System Engineering, 1998, 1(4): 267-284.

[6] Sullivan M J, Oppenheim J, Ahearn M, et al. Defense acquisitions: DoD management approach and processes not-well suited to supports development of global information grid: GAO-06-211[R]. Washington DC: Government Accountability Office, 2006.

[7] 邢栩嘉, 林闯, 蒋屹新. 计算机系统脆弱性评估研究[J]. 计算机学报, 2004, 27(1): 1-11.
Xing Xujia, Lin Chuang, Jiang Yixin. A survey of computer vulnerability assessment[J]. Chinese Journal of Computers, 2004, 27(1): 1-11.

[8] 程正刚, 房鑫炎, 俞国勤, 等. 电力应急体系的脆弱性评价研究[J]. 电力系统保护与控制, 2010, 38(19): 51-54.
Cheng Zhenggang, Fang Xinyan, Yu Guoqin, et al. Research of vulnerability assessment of power emergency system[J]. Power System Protection and Control, 2010, 38(19): 51-54.

[9] 唐士晟, 李小平. 铁路交通事故应急救援体系脆弱性评价方法研究[J]. 铁道学报, 2013, 35(7): 14-20.
Tang Shisheng, Li Xiaoping. Study on method for assessment of vulnerability of railway emergency rescue system[J]. Journal of The China Railway Society, 2013, 35(7): 14-20.

[10] 丁明, 过羿, 张晶晶, 等. 基于效用风险熵权模糊综合评判的复杂电网节点脆弱性评估[J]. 电工技术学报, 2015, 30(3): 214-223.
Ding Ming, Guo Yi, Zhang Jingjing, et al. Node vulnerability assessment for complex power grids based on effect risk entropy-weighted fuzzy comprehensive evaluation[J]. Transactions of China Electrotechnical Society, 2015, 30(3): 214-223.

[11] 张桦, 魏本刚, 李可军, 等. 基于变压器马尔可夫状态评估模型和熵权模糊评价方法的风险评估技术研究[J]. 电力系统保护与控制, 2016, 44(5): 134-140.
Zhang Hua, Wei Bengang, Li Kejun, et al. Research on risk assessment technology based on Markov state evaluation model for power transformer and entropy-weighted fuzzy comprehensive evaluation[J]. Power System Protection and Control, 2016, 44(5): 134-140.

[12] 宁淑婷. 基于二级模糊综合评判的建筑物和桥梁打击效果评估研究[D]. 西安: 西安电子科技大学, 2012.
Ning Shuting. Battle damage assessment of building and bridges based on two-level fuzzy comprehensive evaluation[D]. Xi'an: Xidian University, 2012.

A method for SoS flow vulnerability analysis based on information entropy

WEI Zhengxian[1,2], SONG Min[3*], TONG Pengpeng[4], WANG Hongbin[4]

1. Marine Security System Innovation Center of Science and Technology for National Defense, Beijing 100036, China
2. Pilot National Laboratory for Marine Science and Technology, Qingdao 266011, China
3. Information Technology Center, Beijing Foreign Studies University, Beijing 100089, China
4. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China

Abstract When the system-of-systems (SoS) carries out its missions, it faces various risks of destruction, interference or threat from outside and inside. SoS flow vulnerability is expressed as the degree of impact of mission execution efficiency when a risk event occurs on the SoS flow. In this paper, a method for SoS flow vulnerability analysis based on information entropy is proposed. Firstly, for the risk events and flow structure characteristics, a vulnerability analysis process model is established. Secondly, the SoS flow is transformed into a directed graph model, and a vulnerability calculation model of node in the SoS flow is put forward based on information entropy. Thirdly, the directed graph model of complex SoS flow is decomposed and further simplified to three basic structures: series structure, parallel structure and combination structure, and vulnerability calculation models of these basic structures are also built. Finally, the SoS flow vulnerability can be calculated through the above process. A case study demonstrates the effectiveness of the proposed method.

Keywords information entropy; SoS flow; vulnerability analysis

(责任编辑 刘志远)