DOI:10. 19431/j. cnki. 1673-0062. 2018. 03. 010

基于攻击树的核电厂 DCS 系统信息安全脆弱性分析

赵　庆[1],刘朝晖[1*],陈　智[2]

(1.南华大学 计算机学院,湖南 衡阳 421001;2.中国核动力研究设计院核反应堆系统设计技术重点实验室,四川 成都 610041)

摘　要:随着计算机在核电仪控系统中的广泛运用,其信息安全问题受到越来越大的挑战.提出一种基于攻击树的核电仪控系统信息安全脆弱性分析方法,旨在对系统信息安全脆弱性进行量化分析.该方法首先给叶节点赋予三个不同属性,然后采用模糊层次分析法计算各攻击事件属性的权值.最后计算出叶节点、根节点及攻击路径发生概率.实际案例分析表明:计算得出的结果即给出了各节点和攻击路径发生的概率,还指出了攻击者最有可能采取的攻击路径,证明了该方法是合理可行的.基于攻击树的核电仪控系统信息安全脆弱性分析方法对系统管理者建设防御措施有积极的指导意义.

关键词:攻击树;信息安全;模糊层次分析法;脆弱性分析

中图分类号:TP391　**文献标志码**:B　**文章编号**:1673-0062(2018)03-0054-06

Information Security Vulnerability Analysis of DCS System in Nuclear Power Plant Based on Attack Tree

ZHAO Qing[1], LIU Zhaohui[1*], CHEN Zhi[2]

(1.School of Computer, University of South China, Hengyang, Hunan 421001, China; 2.Key Laboratory of Reactor System Design Technology of Nuclear Power Institute of China, Chengdu, Sichuan 610041, China)

Abstract: Computer is widely used in nuclear power instrumentation and control systems, its information security issues are increasingly challenged. In this essay, an information security vulnerability analysis method for nuclear power control system based on attack tree is proposed to analyze the vulnerability of the system information security. First, the leaf nodes are assigned three different attributes. Then the fuzzy analytic hierarchy process (FAHP) is applied to calculate the weights of the attributes of each attack. Finally, the probability of

收稿日期:2018-01-29

作者简介:赵　庆(1990-),男,硕士研究生,主要从事于计算机网络安全方面的研究.E-mail:729105836@qq.com.*通信作者:刘朝晖(1974-),男,副教授,博士,主要从事于计算机网络安全方面的研究.E-mail:10928478@qq.com

leaf node,root node and attack path are calculated.The actual case analysis shows that the calculated result gives the probability of each node and the attack path,and points out the attack path that the attacker is most likely to take,which proves that the method is reasonable and feasible.The information security vulnerability analysis method of nuclear power plant control system based on attack tree is of positive guidance to the system manager to build the defense measures.

key words:attack tree;information security;fuzzy analytic hierarchy process;vulnerability analysis

0　引　言

我国经济和国家安全相关行业中,工业控制系统起着极其重要的作用.控制系统的功能安全和信息安全在这些行业的生产中起关键作用[1-2].近年来,随着计算机技术在仪控系统中的普遍运用,其带来了大量的信息安全问题,各安全事件也频繁发生,其中核电安全事件尤其引人注意.2010 年爆发了“震网”(Stuxnet)病毒事件,该病毒攻击了伊朗布什尔核电站的系统,导致核设施不能正常运行[3].“震网”病毒引起了全世界对数字化仪控系统信息安全的广泛关注.对此,我国相关部门发布了一系列通知和政策,高度重视信息安全问题.

攻击树模型有结构简单、方法易理解等多种特点,现已应用于许多技术领域,国内外学者已经在安全分析这一领域广泛运用.例如,Ten 等[4]使用攻击树模型对一个 SCADA 系统的信息安全脆弱性进行了评估;Byres 人[5]使用攻击树建模方法对一个基于 Modbus 协议栈的工业控制 SCADA 通信系统进行了漏洞分析.对于判断系统的风险程度,他们只进行定性分析,没有进行定量的分析.李慧等[6]利用攻击树模型对威胁进行建模,用于研究数传电台传输安全性,但是在计算叶子节点发生概率时,缺乏各属性权值算法.黄慧萍等[7]首先利用攻击树对工业控制系统进行建模,再通过概率风险评估技术计算各节点和攻击路径发生的概率,但是该方法没有根据系统特征给出每个安全属性的权值的具体算法.本文采用攻击树模型,利用模糊层次分析法计算各属性的权值,从而定量分析叶节点的发生概率.

1　攻击树模型概念

攻击树(attack tree)模型是 Schneider[8]于 1999 年提出的一种用于分析系统安全的树型结构,对系统可能受到的安全威胁进行分析的方法,它以图形的形式描述各种攻击行为,树的根节点表示攻击者最终攻击目标,叶节点代表攻击者发起的攻击事件.子节点可以称为中间节点,它为上层节点的叶子节点,同时是下层节点的父节点,表示的是实现上层攻击目标的子攻击目标.节点之间连接关系有“与”和“或”两类节点,用图形形式描述攻击树,如图 1 所示,AND 节点为要实现攻击 a 就必须同时实现 b 和 c;OR 节点为 b 和 c 任意一个实现即可实现攻击目标 a.每一条从叶节点到根节点的路径都表示实现此攻击目标开展的一次完整的攻击过程[9].因此,通过遍历整棵攻击树就能够生成攻击根节点的所有的攻击路径.

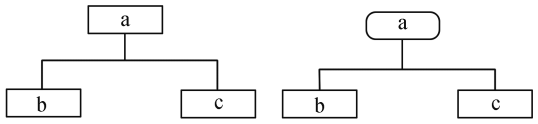

图 1　攻击树 OR、AND 节点表示方法

Fig.1　Attack tree OR,AND node representation method

建立攻击树应考虑许多方面的因素,由相关技术人员认真的分析系统,收集想法提出方案,然后经过反复的推想才能最终建立.首先,将攻击者对系统做的一项安全事件作为根节点,根节点发生必须用到的条件作为子节点,将可能被用到的具体攻击方法或行为作为叶节点,然后按照图 1 方法表示构造一棵或多颗攻击树.从叶子节点到根节点贯穿整个攻击树的路径表示一次具体的攻击过程,即一个攻击序列,最后采用多属性效用理论对叶节点发生概率进行量化,通过分析计算得到的攻击序列,进而找出最大可能被利用的攻击手段.

2 基于攻击树的核电仪控系统信息安全脆弱性分析方法

脆弱性分析的目的就是确定系统存在的漏洞及风险,以及它们被成功利用的概率.利用攻击树模型对系统进行脆弱性分析,其最终目的就是确定由于安全措施在安全方面的不足引起的系统被攻击的概率或风险值.系统技术和管理人员可以依据脆弱性分析结果有针对性地制定安全策略.信息安全脆弱性分析步骤如下:

1)从系统架构、软硬件使用、操作系统、通信协议等多方面分析,确定攻击目标,建立系统攻击树模型;

2)计算叶节点发生概率:首先选择叶节点的属性并量化,其次确定属性的权值,最后根据公式得出叶节点发生概率;

3)计算根节点发生概率;

4)分析计算各攻击路径发生概率,得出最有可能被利用的攻击路径.

2.1 攻击树叶节点的指标量化

通过计算攻击树根节点发生概率就可以得出信息系统存在的危险级别,因而叶节点赋值对系统风险分析很重要,且对计算结果影响很大.攻击者进行相应攻击前往往会综合考虑多个因素,即攻击成本、攻击难度和攻击被发现的可能性等.不同系统对信息安全的侧重点不同,因此给各节点赋予属性值时,这三个属性值的权值并不完全一样.针对这种情况,本文利用模糊层次分析法计算这三个属性对应的权值.

每个节点赋予这三个属性,利用多属性决策方法,将属性转换为实现目标的效用值,计算叶节点发生概率的公式为:

$$P_i = W_{\mathrm{c}} \times U(\mathrm{c}_i) + W_{\mathrm{d}} \times U(\mathrm{d}_i) + W_{\mathrm{f}} \times U(\mathrm{f}_i) \quad (1)$$

其中:i 表示攻击树中的任一叶子节点,即攻击事件;P_i 表示该叶子节点所代表的攻击事件发生的概率;c_i 表示实现此事件的成本;d_i 表示实现的难度等级;f_i 表示该事件可能被发现的等级.W_{c}、W_{d} 和 W_{f} 分别表示这三个属性参数的权重,且权重系数相加等于 1.$U(\mathrm{c}_i)$、$U(\mathrm{d}_i)$ 及 $U(\mathrm{f}_i)$ 分别表示其参数的效用值.

本文以表格的形式制定评分标准,对 P_i 涉及到的三个属性进行评定,如表 1 所示.本文的主要目的是对仪控系统信息安全脆弱性进行量化分析,对于怎样建立评分标准不深入讨论.

表 1 等级评分标准

Table 1 Grading standards

攻击成本(c_i)/万元		攻击难度(d_i)		攻击被发现的可能(f_i)	
攻击成本	等级	攻击难度	等级	被发现的可能性	等级
>15	5	很难	5	很难	1
10~15	4	难	4	难	2
5~10	3	中等	3	中等	3
1~5	2	容易	2	容易	4
<1	1	很容易	1	很容易	5

实际应用的时候,通过专家打分及文献调研的方法给出叶子节点的属性值,由式(1)可知,计算叶子节点发生的概率时,必须知道 $U(\mathrm{c}_i)$、$U(\mathrm{d}_i)$、$U(\mathrm{f}_i)$ 这三个效用值.经过分析得出,c_i、d_i、f_i 与 $U(\mathrm{c}_i)$、$U(\mathrm{d}_i)$、$U(\mathrm{f}_i)$ 成反比的关系,为了便于计算,定义:$U(x) = 1/x$.

2.2 利用模糊层次分析法确定权值

由于层次分析法构造判断矩阵时主观性太强,且矩阵的阶数较大时,计算最大特征根很难,对一致性较差的矩阵还需要反复调整等的缺陷.本文利用层次分析法与模糊综合评判相结合,即模糊层次分析法(FAHP)[10]计算各属性权重.利用 FAHP 计算属性权重步骤有:1)构造模糊判断矩阵,构造矩阵 $\boldsymbol{B}$ 时,b_{ij} 按照模糊矩阵标度表赋予数量标度;2)检验矩阵的一致性,若模糊互补矩阵不具有一致性,对其进行一致性转换,所得矩阵为模糊一致矩阵;3)根据式计算各属性权重,模糊矩阵优先关系数量标度表如表 2 所示.

表 2 模糊矩阵数量标度表

Table 2 Fuzzy matrix number scale table

b_{ij}	含义
0.5	b_i 与 b_j 相比,两者同等重要
0.6	b_i 与 b_j 相比,b_i 比 b_j 稍微重要
0.7	b_i 与 b_j 相比,b_i 比 b_j 明显重要
0.8	b_i 与 b_j 相比,b_i 比 b_j 强烈重要
0.9	b_i 与 b_j 相比,b_i 比 b_j 极端重要
0.1~0.4	若元素 b_i 与元素 b_j 之比为 r_{ij},则元素 b_j 与元素 b_i 之比为 $r_{ji}=1-r_{ij}$

由模糊判断方式对各要素的重要性进行两两

比较,构建判断矩阵 $\boldsymbol{B}$:

$$\boldsymbol{B}\ (b_{ij})_{n\times n}=\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

对模糊判断矩阵进行一致性检验,若对于$\forall i, j, k=1,2,3\cdots n$,满足式(2),则此模糊判断矩阵为模糊一致矩阵.

$$b_{ij}=b_{ik}-b_{jk}+0.5 \tag{2}$$

否则,对模糊互补判断矩阵 $\boldsymbol{B}(b_{ij})_{n\times n}$ 按行求和得 r_i, 再用式(4)进行转换.

$$r_i=\sum_{k=1}^{n} r_{ik}(i=1,2,\cdots,n) \tag{3}$$

$$r_{ij}=\frac{r_i-r_j}{2n}+0.5 \tag{4}$$

由式(2)~(4)完成模糊一致转换,所得模糊一致判断矩阵为 $\boldsymbol{R}=(r_{ij})_{n\times n}$. 计算权重值时有多种方法,本文采用最小二乘法计算属性的权值[11].用式(5)计算各属性的权值.

$$W_i=\frac{1}{n}-\frac{1}{2a}+\frac{1}{na}\sum_{j=1}^{n} r_{ij}(i=1,2,\cdots,n) \tag{5}$$

式(5)中参数 $a\geqslant(n-1)/2$,a 大小与权重之间的差异度成反比.由此,可以利用 a 来进行权值结果分析,然后根据分析选择最适合的权值,本文 a 的取值为$(n-1)/2$.

2.3　计算根节点发生概率

攻击者最终目标是使一个攻击序列成功发生,即成功攻击根节点,从而达到最终目的.首先遍历整棵攻击树确定攻击路径,然后通过攻击路径和叶节点发生概率计算出根节点发生概率.

从攻击树模型特性分析,有两种情况求父节点发生概率,即 AND 节点和 OR 节点.

1)对于 AND 节点:$P(G)=P(G_1)\times P(G_2)\times\cdots\times P(G_n)$

2)对于 OR 节点:$P(G)=\max\{P(G_1),P(G_2),\cdots,P(G_n)\}$

$P(G)$ 为父节点发生概率;G_i 为子节点,$P(G_i)$为子节点 G_i 发生的概率.

任何一条从叶节点的攻击事件到根节点的攻击目标的实现,都代表发生了一次攻击路径[12],据 AND 节点和 OR 节点,从底到上遍历整颗攻击树确定所有攻击路径.假设 S_i 为一条攻击路径,$S_i=(X_1,X_2,X_3,\cdots,X_n)$,$X_i$ 表示叶子节点.则攻击路径 S_i 发生的概率为:$P(S_i)=\prod_{i=1}^{n}P(X_i)(i=1,2,\cdots,n)$. 根据上面公式计算出每条攻击路径发生的概率,概率越大越容易被利用,然后根据计算结果采取相应的防范措施.

3　实际案例分析

本部分利用攻击树模型对某个核电厂安全级 DCS 平台进行信息安全脆弱性分析.该平台分为现场控制站、传输站、安全显示站、网关站和工程师站,除网关站和工程师站外均属于核安全级(1E 级)设备.其中,现场控制站完成信号采集、数据处理、逻辑运算,信号输出和数据通信功能,传输站承担现场控制站和安全显示站、网关站和工程师站的数据接口功能,安全显示站是该平台的人机接口,实现安全级过程参数及报警显示、设备控制机复位闭锁等功能,网关站实现该平台和外部非安系统的数据交互,工程师站主要实现组态、下装和维护等功能,平台基本架构如图 2 所示.

建立攻击树模型对该平台进行详细脆弱性分析,并根据分析得出的威胁和漏洞提出与之对应的防范措施.对该平台系统的攻击可以分解为 G_1:攻击现场控制站、G_2:攻击工程师站、G_3:攻击安全显示站、G_4:攻击网关站、G_5:攻击传输站.其中这五个子攻击目标中任意一个被成功攻击,都会给整个平台带来严重危害.

由于核电厂 DCS 系统要求高保密性,所以攻击难度这个属性的重要性最高,攻击被发现的可能性和攻击成本的重要性依次降低.根据表 2 构造模糊互补判断矩阵 $\boldsymbol{B}$:

$$\boldsymbol{B}=\begin{bmatrix} 0.5 & 0.6 & 0.7 \\ 0.4 & 0.5 & 0.6 \\ 0.3 & 0.4 & 0.5 \end{bmatrix}$$

通过式(2)对矩阵 $\boldsymbol{B}$ 进行一致性检验,检验结果为矩阵 $\boldsymbol{B}$ 满足模糊一致矩阵的性质.也就是说,矩阵 $\boldsymbol{B}$ 为模糊一致矩阵,不用再对其进行转换.由式(5)计算得出 $W=[0.433,0.333,0.234]$,即权重值 $W_{\mathrm{d}}=0.433$,$W_{\mathrm{f}}=0.333$,$W_{\mathrm{c}}=0.234$.将计算得出的属性权值及参数效用值代入式(1)即可计算出叶节点发生的概率.

下面以攻击现场控制站为例构造攻击树模型.如图 3 所示,该攻击树各节点含义如表 3 所示.

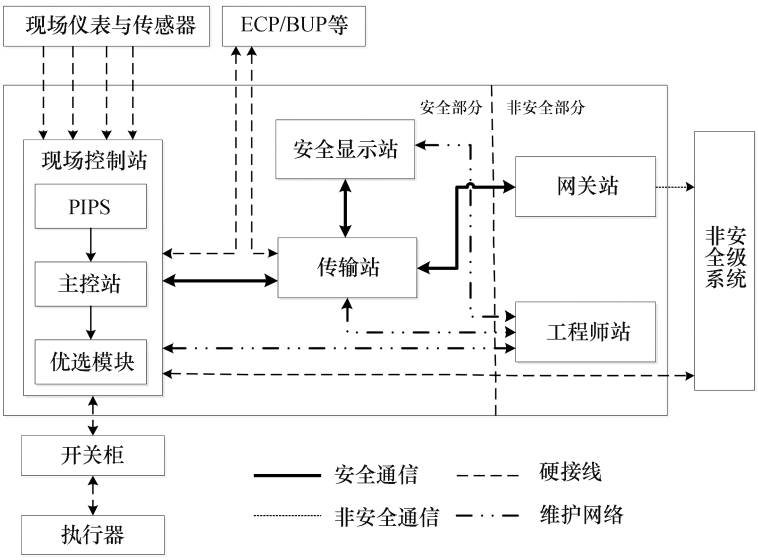

图 2 某平台基本架构和组成示意图

Fig.2 Basic architecture and schematic diagram of the platform

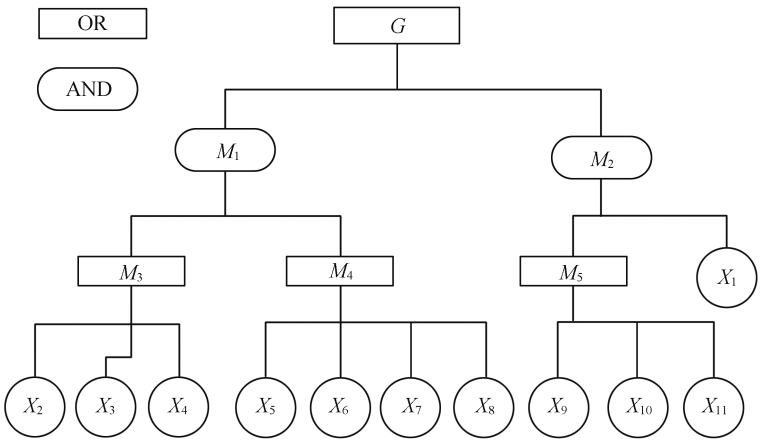

图 3 现场控制站攻击树模型

Fig.3 The attack tree model of field control station

表 3 攻击树中各个节点的含义

Table 3 The meaning of each node in the attack tree

节点	含义	节点	含义
G	攻击现场控制站	X_4	站间通信网络接入
M_1	攻击控制器	X_5	写入非法程序
M_2	攻击通信网络	X_6	修改配置参数
M_3	非法接入设备	X_7	改变控制器状态(启、停)
M_4	进行攻击	X_8	其他攻击(读、写数据)
M_5	攻击网络	X_9	读、写实时数据
X_1	非法接入预留通信接口	X_{10}	截取或修改数据
X_2	预留编程接口接入	X_{11}	阻塞网络
X_3	工程师站维护端口接入		

采用表 1 评分标准,由专家对现场控制站攻击树中各个叶子节点的三个属性进行模糊评分,对每个叶子节点评分结果进行统计,如表 4 所示.

表 4 各叶节点属性得分

Table 4 Attribute score of each leaf node

叶节点	攻击成本	攻击难度	被发现可能性	叶节点	攻击成本	攻击难度	被发现可能性
X_1	3	4	3	X_7	3	4	5
X_2	3	4	4	X_8	3	3	4
X_3	2	3	3	X_9	3	4	2
X_4	3	5	2	X_{10}	3	4	2
X_5	2	3	4	X_{11}	2	3	2
X_6	2	3	4				

由上述方法计算出叶子节点的属性权值,根据属性的权值以及表 4 中各值,由式(1)计算出

每个叶节点发生概率,计算结果如表 5 所示.

表 5　叶节点发生概率

Table 5　Occurrence probability of leaf node

攻击	发生概率	攻击	发生概率	攻击	发生概率
X_1	0.297	X_5	0.345	X_9	0.353
X_2	0.270	X_6	0.345	X_{10}	0.353
X_3	0.372	X_7	0.253	X_{11}	0.428
X_4	0.331	X_8	0.310		

由图 3 分析可知,实现攻击树的最终攻击目标共有 15 种攻击路径.具体如下所示:$S_1=(X_2,X_5)$、$S_2=(X_2,X_6)$、$S_3=(X_2,X_7)$、$S_4=(X_2,X_8)$、$S_5=(X_3,X_5)$、$S_6=(X_3,X_6)$、$S_7=(X_3,X_7)$、$S_8=(X_3,X_8)$、$S_9=(X_4,X_5)$、$S_{10}=(X_4,X_6)$、$S_{11}=(X_4,X_7)$、$S_{12}=(X_4,X_8)$、$S_{13}=(X_1,X_9)$、$S_{14}=(X_1,X_{10})$、$S_{15}=(X_1,X_{11})$.利用式 $P(S_i)=\prod_1^n P(x_i)$ $(i=1,2,\cdots,n)$ 计算各攻击路径发生概率,如表 6 所示.

表 6　各攻击路径发生概率

Table 6　Occurrence probability of each attack path

攻击	发生概率	攻击	发生概率	攻击	发生概率
S_1	0.093	S_6	0.128	S_{11}	0.085
S_2	0.093	S_7	0.094	S_{12}	0.103
S_3	0.068	S_8	0.115	S_{13}	0.105
S_4	0.084	S_9	0.114	S_{14}	0.105
S_5	0.128	S_{10}	0.114	S_{15}	0.127

分析表 7 可知,攻击路径 S_5、S_6、S_{15}在现场控制站攻击树模型中发生的概率较大,即攻击事件是(X_3,X_5)、(X_3,X_6)、(X_1,X_{11}).可以说,攻击者非常有可能通过工程师站接入非法设备来攻击控制器,从而达到攻击现场控制站的目的.另一可能就是,攻击者通过网络通信接口发送大量的无用数据来阻塞网络,以此达到攻击现场控制站的目的.因此,应有针对性的制定防范错略和保护措施.

利用上述方法对另外四个子攻击树进行脆弱性分析,即可得到 5 项量化的数据,由此可以得出整个该平台脆弱性分析结果.对于较为严重的几个攻击路径,由相关部门和技术人员制订方案、部署防御措施,加强保护来减少其对系统造成的危害.

4　结　论

本文提出采用攻击树模型对核电 DCS 系统进行脆弱性分析,计算攻击事件发生概率过程中,先对叶节点进行指标量化,其次利用 FAHP 方法计算属性权值,最后以实例计算分析系统脆弱性.在计算各属性权重时引入模糊一致矩阵,一定程度克服了层次分析法主观性太强,缺乏模糊性的缺陷,但仍受主观因素的影响.下一步工作重点是如何降低主观因素对系统脆弱性分析的影响,考虑建立攻击事件发生概率的影响因素库,可以采用神经网络来预测叶节点发生的概率.

参考文献:

[1] GREERY A, BYRES E. Industrial cyber security for a power system and SCADA networks[J]. IEEE industry applications, 2007, 13(4): 49-55.

[2] IGURE V, LAUGHTER S, WILLIAMS R. Security issues in SCADA networks[J]. Computers and security, 2006, 25(7): 498-506.

[3] 魏钦志.工业网络控制系统的安全与管理[J].测控技术,2013,32(2):87-92.

[4] TEN C W, LIU C C, GOVINDARASU M. Vulnerability assessment of cybersecurity for SCADA system using attack trees[J]. IEEE Power engineering society general meeting, 1932, 23(4): 1-8.

[5] BYRES E J, FRANZ M, MILLER D. The use of attack trees in assessing vulnerabilities in SCADA systems[C]// Proceedings of the international infrastructure survivability workshop citeseer, 2004: 3-10.

[6] 李慧,张茹,刘建毅,等.基于攻击树模型的数传电台传输安全性评估[J].信息网络安全,2014(8):71-76.

[7] 黄慧萍,肖世德,孟祥印.基于攻击树的工业控制系统信息安全风险评估[J].计算机应用研究,2015,32(10):3022-3025.

[8] SCHNEIER B. Attack tress modeling security threats[J]. Dr.dobb's journal, 1999, 24(12): 21-29.

[9] 王华忠,颜秉勇,夏春明.基于攻击树模型的工业控制系统信息安全分析[J].化工自动化及仪表,2013,40(2):219-221.

[10] 张吉军.模糊层次分析法(FAHP)[J].模糊系统与数学,2000,14(2):80-88.

[11] 兰继斌,徐扬,霍良安,等.模糊层次分析法权重研究[J].系统工程理论与实践,2006,26(9):107-112.

[12] 夏丹阳,徐展,向媛,等.反应堆保护系统信息安全分析[J].核电子学与探测技术,2016,36(11):1103-1107.

(责任编辑:龙威)