中国电子信息产业发展研究院
赛迪工业和信息化研究院（集团）有限公司 主办

ISSN 2095-8412
CN 10-1231/F

工业技术创新

Industrial Technology Innovation

CCID 赛迪出版物

2022年第5期 10月25日出版 总第52期

高炉炉热闭环智能控制系统研究与应用评价

基于机器视觉的五金行业自动化组装生产线系统研究

沸石—地聚合物复合多孔材料制备及其二氧化碳吸附性能研究

利用Izhikevich模型探究神经元动作电位的发放特性

MOEA/D算法在扩展互作用振荡器优化设计中的应用研究

ISSN 2095-8412

9 772095 841226 10>

原国家新闻出版广电总局第一批认定学术期刊
《中国学术期刊评价研究报告》（第6版）认定“RCCSE中文学术期刊”
本刊已被以下期刊数据库收录：
国家哲学社会科学学术期刊数据库
国家哲学社会科学文献中心
国家科技期刊开放平台
中国科学引文索引（CSCI）
中国知识资源总库（CNKI）
中国核心期刊（遴选）数据库

面向对象的Petri网智能工厂资产风险评估模型及应用研究

王佳，赵文苹，秦嘉言
（中国软件评测中心，北京 100048）

摘 要： 风险评估是识别智能工厂资产风险，保障数字化制造企业资产安全运营的有效策略。围绕智能工厂资产系统结构中的资产价值、威胁和脆弱性要素，提出资产价值、资产安全风险值的评估策略。采用有序加权几何平均（OWGA）算子，有效集结数据信息，对资产重要性进行排序，从而通过资产、风险概率、威胁后果等权重的计算，对安全风险进行排序，提高资产风险评估的客观性和可度量性。考虑资产之间的信息传递，辅以安全特征分析，形成风险评估流程，采用顺序、共同、并发、继发4种资产相互影响的关系形式，建立了资产识别、威胁识别和安全策略识别的Petri网拓扑结构。实例分析表明，这一模型能够指导智能工厂等复杂系统利用资产重要性、风险概率、威胁后果等参数特征，设计相应的安全防护措施，保障资产管理和运维水平。

关键词： 智能工厂；风险评估；Petri网；有序加权几何平均（OWGA）；复杂系统
中图分类号： TP277 **文献标识码：** A **文章编号：** 2095-8412 (2022) 10-019-09
工业技术创新 URL: http://gyjs.cbpt.cnki.net DOI: 10.14103/j.issn.2095-8412.2022.10.003

0 引言

随着制造业数字化转型的深入推进，工厂资产管理逐渐转变为朝着智能化等方向发展，资产安全问题在智能工厂生产场景中日益深化，拦截等传统安全防护方式已无法应对新形势下的安全挑战。运用风险评估策略识别资产安全风险，有针对性地保护智能工厂现场设备，受到了广泛的重视[1-2]。

风险评估与其他方法一样，可分为定性分析方法和定量分析方法。定性分析方法包括基于标准的内容分析（Criteria-Based Content Analysis，CBCA）、工艺危害分析（Process Hazards Analysis，PHA）和危害与可操作性分析（Hazards and Operability Analysis，HAZOP）等[3]，这些方法过度依赖专家经验知识和评估标准的准确性。典型的定量分析方法包括聚类分析法、决策树法等，这些方法也受到人为操作等因素的影响。知识推理方法是一种定性分析与定量分析相结合的方法，包括层次分析法、故障树和攻击图等，能够较为客观地为系统安全状态提供分析，但需要以较多的先验知识为保障，限制了其在大规模风险评估环境中的应用[4-6]。

Petri网是一种运用图形化能力和数学定义对事件或事物之间的依赖关系进行表示的模拟和分析工具，在系统机理重现和评价中受到了广泛应用[7-9]。但是，智能工厂资产风险评估复杂度较高，采用传统的Petri网对这一复杂系统进行建模，会出现状态空间爆炸问题。采用面向对象的Petri网，将每一个资产映射为与其他资产相互协作的对象，可显著降低模型复杂度，提高Petri网的威胁路径搜索效率。

由于智能工厂资产风险因素非常多，且各因素之间相互影响，因此识别关键风险因素并判断其重要程度，成为智能工厂资产风险评估的首要问题。本文首先按照制造企业功能层次模型，刻画智能工厂资产系统结构；然后，围绕资产价值、威胁和脆弱性等基本要素，构建面向对象的Petri网智能工厂资产风险评估模型，形成智能工厂资产风险评估基本流程；最后，开展实例分析，以直观的图形表示资产价值评估、资产风险识别和资产安全策略识别的Petri网模型，进一步凸显智能工厂资产风险评估

工业技术
Industrial Technolog
2022年第5期
(Gongye Jishu Chu
主管单位：中华人民共和
主办单位：中国电子信息
赛迪工业和信
出版单位：北京赛迪出版
主　　编：张　阔
责任编辑：吕红秋
美术编辑：吴　桐
编辑电话：010-8855890
发行单位：北京赛迪出版
订阅热线：010-8855877
传　　真：010-88558850
主　　页：gyjs.cbpt.cn
邮　　箱：gyjscx@ccidr
出版日期：2022年10月25
广告发布登记：京海工商广
承　　印：廊坊市鸿煊印刷
编辑出版地址：北京市海淀

的理论逻辑和应用逻辑。

1 智能工厂资产系统结构

按照制造企业功能层次模型进行划分，各个功能层级包括的主要资产有工业设备、自动化控制系统、工业网络、应用软件，如图1所示。

工业设备主要有工控机、编程逻辑控制器（Programmable Logic Controller，PLC）、智能仪器仪表、智能传感器等产品，工业设备安全是智能工厂资产安全的基础。自动化控制系统主要有数据采集与监视控制系统（Supervisory Control and Data Acquisition，SCADA）、分散控制系统（Distributed Control S
系统（Manufacturing E
工程师站等，这些系统
平台软件的健壮性以及
工厂资产安全的支撑。
网络、外部的信息网络
机、路由器、网闸、防
资产安全的前提。应用
业务功能，是智能工厂
资产被攻击，安全运维
量的损失。因此，加强
估水平和资产运维水平
持续发展的核心任务[

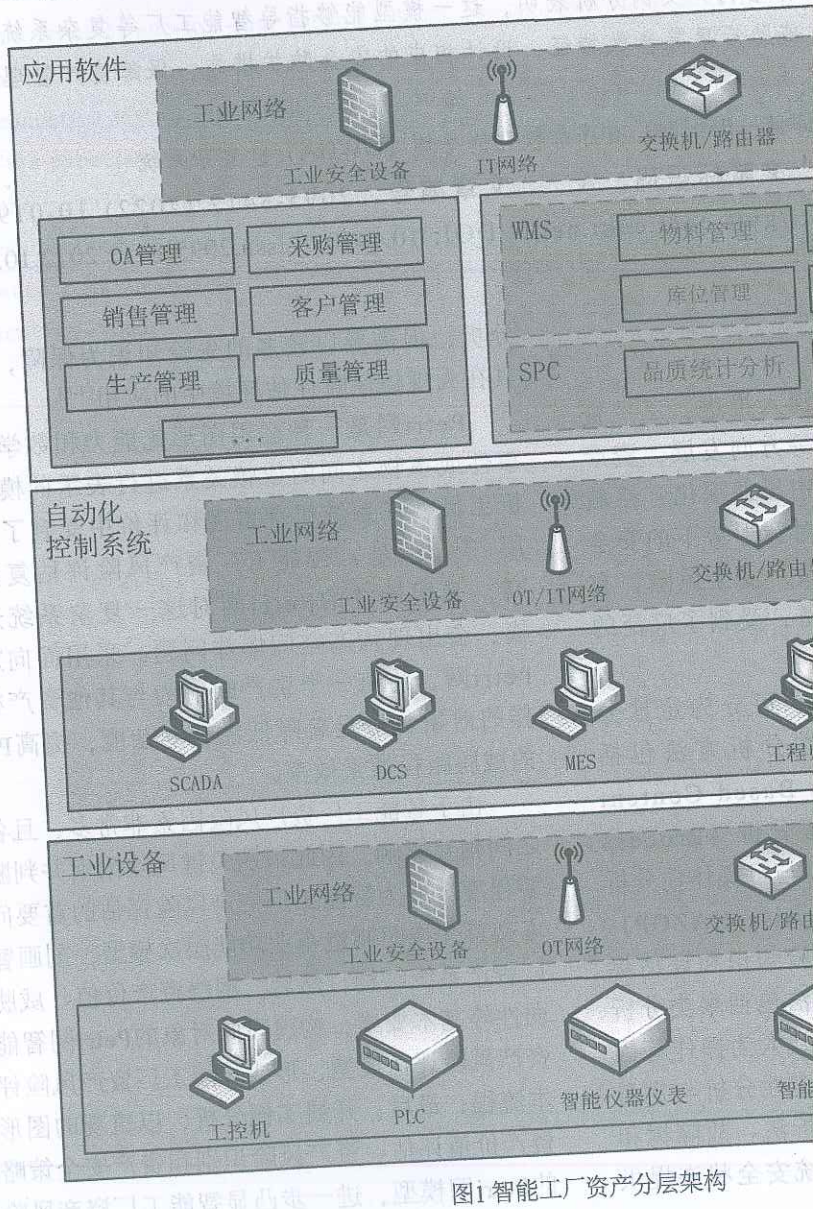


图1 智能工厂资产分层架构

2 基本要素分析

风险评估主要是根据相关标准和技术，围绕资产价值、威胁和脆弱性对资产可能面临的安全问题进行的评估[11-13]。本章结合智能工厂特点，对上述基本要素进行分析。

2.1 资产价值评估

资产价值评估的作用主要是识别资产和对资产赋值。不同资产存在的弱点、面临的威胁、受到保护的程度和安全控制机制各不相同。智能工厂IT系统和工业控制系统虽然均以资产机密性、完整性、可用性为目标，但三者的优先级也有差异，主要区别如图2所示。

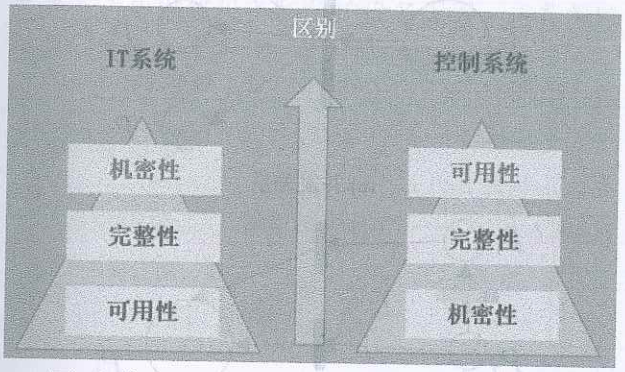


图2 智能工厂IT系统和工业控制系统机制差异分析

传统风险评估方法没有根据机密性、完整性、可用性这三个要素对资产重要性进行分级和排序。在本文提出的风险评估模型中，资产价值由这三个要素综合计算确定[14]。资产重要性判断准确与否，直接事关风险评估结果的正确性。有序加权几何平均（OWGA）算子是一种有效集结数据信息，并对资产重要性进行排序的方法，其定义如下。

定义 若$\mathrm{OWGA}_w(a_1,a_2,\cdots,a_n)=\prod_{j=1}^{n}b_j^{w_j}$，则$\mathrm{OWGA}:R^{+^n}\to R^+$。其中，$w=(w_1,w_2,\cdots,w_n)$是与OWGA相关联的指数加权向量，$w_j\in[0,1]$，$j\in\mathbf{N}$，$\sum_{j=1}^{n}w_j=1$；$b_j$是一组数据$(a_1,a_2,\cdots,a_n)$中第$j$大的元素；$R^+$为正实数集。

2.2 资产安全风险值（威胁和脆弱性）评估

资产安全风险值评估考虑了威胁发生可能性与后果的结合效果。风险由威胁引起，威胁利用脆弱性来危害资产，其中脆弱性反映漏洞情况及安全策略配置情况。威胁越大，风险越大；脆弱性越大，风险也越大。

在智能工厂资产风险评估中，威胁是对智能工厂资产危害程度的度量。常见的威胁包括管理漏洞、物理环境设施、软硬件故障、恶意代码和病毒、黑客攻击等[14-15]，其说明如表1所示。

特定威胁产生的后果属性是不同的，并且是有权重的，取决于不同威胁后果的严重程度以及系统对不同威胁的承受能力，考虑因素一般包括收入损失、对生产力的损害、对公共信誉的损害。

根据智能工厂资产实际情况，首先确定威胁后果的属性类型，即哪些方面对系统造成安全损害；然后评估威胁对系统的危害程度，充分考虑不同后果的属性权重，得到被评估对象实际的安全风险。将威胁后果表示为$X:\{x_j|j=1,2,\cdots,m\}$，其中x_j为第j种后果，m是威胁后果种类数量；威胁后果

表1 常见的威胁及其说明

威胁名称	说明
管理漏洞	违反法律、法规和相关的标准；不符合公司或行业的安全管理制度；不符合企业的安全操作程序、规定
物理环境	断电、静电、湿度、温度、电磁干扰、洪灾、火灾、地震等环境问题和自然灾害
软硬件故障	硬件产品故障，网络通信中断、系统本身或软件bug导致业务系统的破坏和故障
恶意代码和病毒	病毒一般都具有自我复制的功能，同时，它们还可以把自己的副本分发到其他文件、程序或电脑中，破坏电脑数据，运行具有入侵性或破坏性的程序，损害电脑数据的安全性和完整性
黑客攻击	通常采用拒绝服务攻击或信息炸弹；实施破坏性攻击，侵入他人电脑系统，盗窃系统保密信息，破坏目标系统的数据

相应的权重表示为$W:\{w_j|j=1,2,\cdots,m\}$，其中w_j为第j种后果的权重。

在确定好威胁后果属性和权重后，对每种威胁发生的可能性和可能造成的后果值进行分析。通过历史数据确定威胁发生概率$P:\{p_i|i=1,2,\cdots,n\}$及其相应资产安全风险值集合$V_{ij}:\{v_{ij}|i=1,2,\cdots,n;j=1,2,\cdots,m\}$。其中，$v_{ij}$为威胁在后果$x_j$上可能造成的风险值。

由于威胁对系统造成的后果影响是多方面的，为度量方便，统一度量标准，消除量纲的影响，得到威胁在后果x_j上造成的相对后果，即

$$V_{ij}^{*}=\frac{v_{ij}}{\max_{k=1}^{n}(V_{ij})} \tag{1}$$

其中，$\max_{k=1}^{n}(V_{ij})$是威胁后果所造成的威胁影响的最大值。

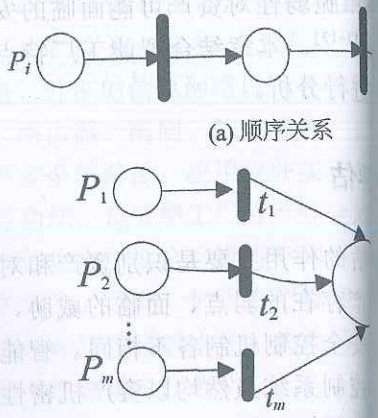
风险评估不是为了确定威胁的严重程度，而是为了度量和比较各个威胁的相对严重程度，从而选择所需的风险控制类型，采取相应的安全决策，即利用V_{ij}^{*}对各类风险进行排序，然后根据风险等级采取相应措施。

3 Petri网构建及风险评估流程设计

3.1 Petri网构建

Petri网是一种网状信息流模型，结构元素包括库所（Place）、变迁（Transition）和有向弧（Arc）。库所是表示状态的元素，描述系统局部状态。变迁是表示变化的元素，描述改变系统状态的事件。有向弧表示状态和事件之间的流关系。因此，可以根据Petri网的基本概念，建立智能工厂资产Petri网模型，描述各个资产相互影响的过程[16-17]。

智能工厂资产之间相互影响，一般包括顺序关系、共同关系、并发关系以及继发关系，如图3所示。顺序关系用于描述活动之间的诱发关系（图3a）。共同、并发主要用于描述资产在不同层次单元下风险状态传递的情况，其中共同关系表示多个低层次资产共同影响高层次资产，并实现相应功能（图3b），并发关系表示低层次连接资产或者与其他多个高层次资产联系密切的单元，会同时导致与之相联系的多个资产风险（图3c）。继发关系主要用于描述同层状态的影响，以及其进而对高层次态产生的影响（图3d）。



(a) 顺序关系

(b) 共同关系

(c) 并发关系

(d) 继发关系

图3 智能工厂资产之间相互

资产风险是在不同事件驱动全状态、脆弱状态和危险状态的。在威胁攻击下，资产如果有得到合适的安全保护，就会在受到无效威胁引起的攻击时全状态。由Petri网建立的资型，能够完整、准确描述资产性）和保护措施之间的基本关有资产进行表达后，即可通过传播路径进行描述，对安全风通过推理方法快速定位风险源风险在线诊断分析提供有效途

工业技术
Industrial Technol
2022年第
(Gongye Jishu
单位：中华人民共
单位：中国电子信
赛迪工业和
单位：北京赛迪出
编：张 阔
编辑：吕红秋
编辑：吴 桐
电话：010-88558
单位：北京赛迪出
热线：010-88558
真：010-885588
页：gyjs.cbpt.c
箱：gyjscx@cci
期：2022年10月
布登记：京海工商
印：廊坊市鸿煊印
版地址：北京市海

3.2 风险评估流程设计

对智能工厂资产风险评估模型进行构建后，考虑资产之间的信息传递，辅以安全特征分析[18]，形成风险评估流程，如图4所示。

具体步骤：

（1）风险评估准备。对智能工厂中各个资产系统进行分析，考虑机密性、完整性、可用性等属性，给出资产评价，并建立资产识别Petri网模型。按照智能工厂中各个系统之间的层次和信息流动关系，构造出各个资产之间的消息传递关系。

（2）综合考虑资产价值、威胁、脆弱性，进行风险价值评估，为智能工厂资产建立威胁识别、安全策略识别Petri网模型。

（3）对资产进行响应处置。根据资产重要性和资产风险分析结果确定优先级，然后通过资产自身及边界网络设备和防护设备配置，进行策略调整，依据整体保护框架，制定安全方案。

4 实例分析

假设智能工厂中有两个资产——A1和A2。对资产安全现状进行调研得知，资产的威胁包括管理漏洞、物理环境、软硬件环境、恶意代码和病毒、黑客攻击等。在资产风险评估中需要考虑的因素包括：资产价值，即通过OWGA集结得到的不同资产的价值程度；威胁发生的概率，由历史统计值来确定；资产脆弱性的严重程度，利用漏洞扫描工具获取。

决策者首先对设备的机密性、完整性和可用性进行赋值（范围1~5），由资产{机密性、完整性、可用性}集合，得到资产A1、A2的三个不同属性的赋值分别为{3,4,2}和{4,3,3}。利用OWGA算子，假设w=(0.5, 0.3, 0.2)，对机密性、完整性和可用性属性值进行集结，得到决策者所给出的资产的综合属性值。资产A1=$4^{0.5}\times3^{0.3}\times2^{0.2}$=3.17；资产A2=$4^{0.5}\times3^{0.3}\times3^{0.2}$=3.44。资产A1<资产A2，即资产A2重要性大于资产A1。

根据Petri网建模流程，建立资产A2的资产识别Petri网模型，如图5所示。其中，P1—资产分类评估信息；T1—资产重要性识别分析；P11—机密性属性；P12—完整性属性；P13—可用性属性；T11—机密性受破坏影响分析；T12—完整性受破坏影响分析；

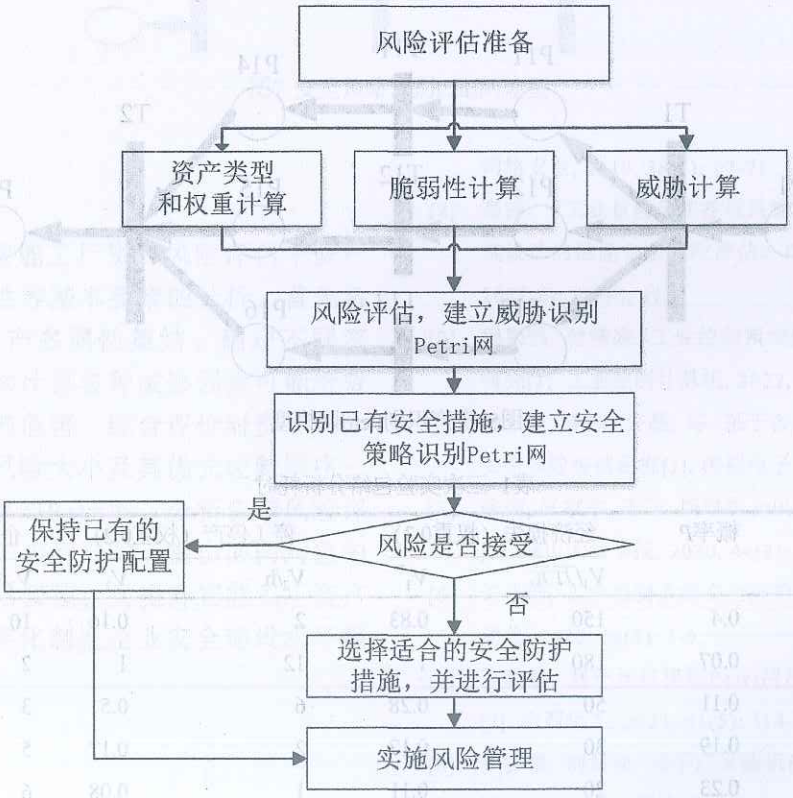


图4 风险评估流程

P14—机密性受破坏影响分析结果；P15—完整性受破坏影响分析结果；P16—可用性受破坏影响分析结果；T2—资产受破坏产生的影响综合分析；P2—资产属性受破坏产生的影响综合分析。

对资产受到的威胁进行分析，确定威胁类别包括管理漏洞威胁、物理环境威胁、软硬件环境威胁、恶意代码和病毒、黑客攻击。这些威胁可能给企业带来经济损失、停工停产以及危害企业信誉等危害，该企业认为危害企业信誉的危害性最大。针对被评估资产A2的历史数据，确定风险概率和威胁后果值如表2所示。从表2中分析可知，该资产由于管理漏洞造成信息系统故障或损害发生的概率最大，其次是黑客攻击、恶意代码和病毒。造成损失收入最大的威胁是物理环境威胁，造成停工停产最大的威胁是物理环境威胁，造成企业信誉损失最严重的威胁是黑客攻击。

接收上一过程工厂资产识别信息，建立威胁识别Petri网模型，如图6所示。其中，IM21—接收资产价值信息；T31—分析威胁源；P3—威胁源列表；T32—威胁源分类；P30—管理漏洞威胁；P31—物理环境威胁；P32—软硬件环境威胁；P33—恶意代码和病毒；P3
管理漏洞威胁分析；T33—
T34—软硬件环境威胁分析
毒威胁分析；T36—黑客攻
理漏洞威胁行为列表；P36
P37—软硬件环境威胁列表
毒威胁列表；P39—黑客攻
—威胁识别结果综合；P4—

根据识别资产的安全要
别Petri网模型，如图7所示
资产价值信息；IM41—接
胁利用的脆弱性信息；T5
险评估结果；T52—根据风
定的安全要求；P52—系统
—记录资产的安全要求；C
略信息。

在实际应用中，风险评

通过IM21和IM41接收
风险信息，作为风险评估的
法，计算系统的某个或多个
小，从而采取相应的安全措

在对资产进行风险评

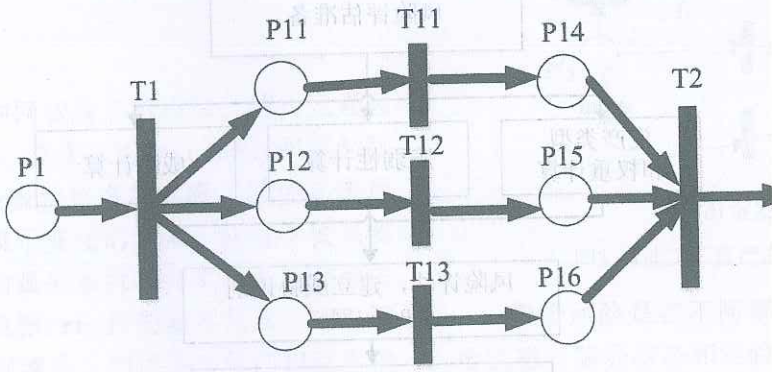


图5 资产识别Petri网模型

表1 三次实验包络分析耗时

威胁名称	概率P	经济损失（权重0.3）		停工停产（权重0.2）	
		V_1/万元	V_1^*	V_2/h	V_2^*
管理漏洞	0.4	150	0.83	2	0.16
物理环境	0.07	180	1	12	1
软硬件环境	0.11	50	0.28	6	0.5
恶意代码和病毒	0.19	30	0.17	2	0.17
黑客攻击	0.23	20	0.11	1	0.08

工业技
Industrial Techn
2022年
(Gongye Jish
主管单位：中华人民
主办单位：中国电子
赛迪工业
出版单位：北京赛迪
主　　编：张　阔
责任编辑：吕红秋
美术编辑：吴　桐
编辑电话：010-885
发行单位：北京赛迪
订阅热线：010-8855
传　　真：010-8855
主　　页：gyjs.cbpt
邮　　箱：gyjscx@c
出版日期：2022年10
广告发布登记：京海工
承　　印：廊坊市鸿煌
编辑出版地址：北京市

的风险和采取的安全策略为：

（1）用户标识不唯一，存在被恶意用户非法操作的风险，应对资产A2中的用户进行身份唯一标识和鉴别；

（2）资产系统密码复杂度不符合要求，应在管理层面规定密码的复杂度和并定期更换；

（3）资产易受到木马攻击，应安装防恶意代码软件，及时更新软件版本和恶意代码库。

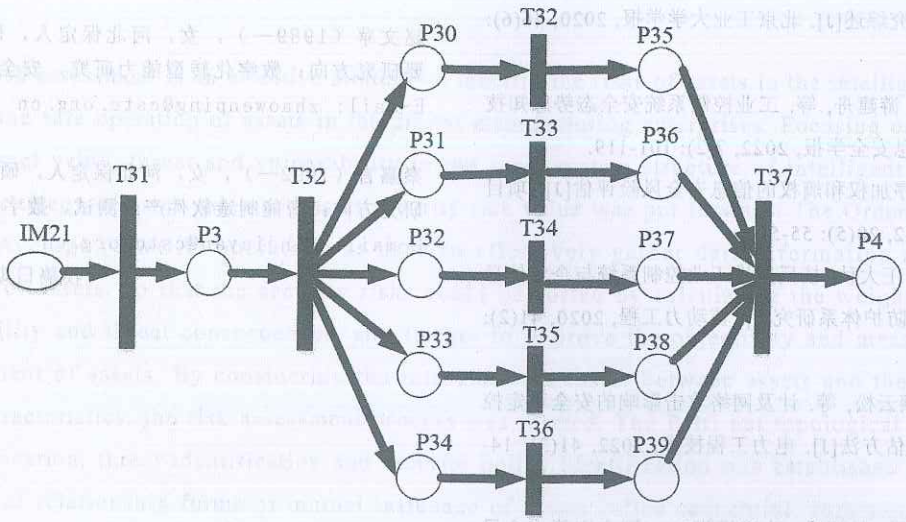


图6 威胁识别Petri网模型

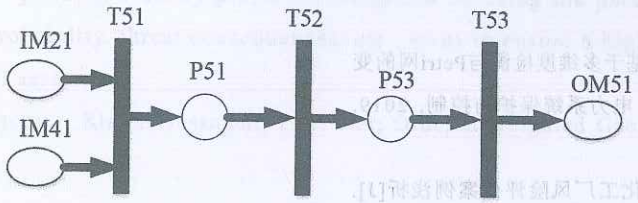


图7 安全策略识别Petri网模型

5 结束语

本文立足于对智能工厂资产风险评估中资产价值、威胁和脆弱性等基本要素的分析，首先将OWGA算子用于资产多属性集结，确定不同资产的重要程度；其次计算各种威胁因素可能给资产带来的不同层面的危害，综合评价对资产产生的风险，确定安全风险大小及其优先控制顺序；最后，借助面向对象的Petri网，分析资产风险评估在Petri网模型中的表现形式，提出面向对象的Petri网资产风险评估模型，为提升智能工厂资产管理能力，提高数字化制造企业安全建设水平提供了一种新的思路。

参考文献

[1] 黄兆军. 智能工厂工控系统安全风险评估[J]. 信息技术与网络安全, 2019, 38(3): 67-71.

[2] 高涛. 《工业自动化和控制系统的安全性—第3-2部分：系统设计的信息安全风险评估》标准解析[J]. 中国标准化, 2022(6): 89-96, 111.

[3] 魏振强, 付晓晓. 工业控制系统安全防护一体化风险评估研究[J]. 工业控制计算机, 2022, 35(1): 5-6, 9.

[4] 杨黎霞, 李杰, 许磊, 等. 基于多属性决策的工业控制系统安全风险评估研究[J]. 消费电子, 2022(3): 90-92.

[5] 张炳, 任家东, 王苎. 网络安全风险评估分析方法研究综述[J]. 燕山大学学报, 2020, 44(3): 290-305.

[6] 许光泞. 工业控制系统安全防护体系研究[J]. 石油化工自动化, 2020, 56(3): 1-6.

[7] 张晓静. 基于加权模糊Petri网的化工安全风险评估方法[J]. 山西化工, 2021, 41(5): 114-115, 119.

[8] 黄祎铁, 刘君强. 基于广义随机Petri网的机场滑行道风险研究[J]. 航空计算技术, 2022, 52(1): 55-59.

[9] 余建星, 曾庆泽, 余杨, 等. 基于模糊Petri网络的FPSO单点多管缆干涉风险评估[J]. 海洋工程, 2022, 40(1): 10-20.
[10] 黄兆军. 智能工厂的工业控制系统网络安全防御体系的构建[J]. 工业技术与职业教育, 2019, 17(2): 5-10, 18.
[11] 赖英旭, 刘静, 刘增辉, 等. 工业控制系统脆弱性分析及漏洞挖掘技术研究综述[J]. 北京工业大学学报, 2020, 46(6): 571-582.
[12] 周明, 吕世超, 游建舟, 等. 工业控制系统安全态势感知技术研究[J]. 信息安全学报, 2022, 7(2): 101-119.
[13] 王蔚. 基于有序加权和熵权的信息安全风险评估[J]. 项目管理技术, 2022, 20(5): 55-59.
[14] 秦利华, 王丹, 王大秋. 核反应堆工业控制系统与企业信息系统互联安全防护体系研究[J]. 核动力工程, 2020, 41(2): 173-177.
[15] 钱胜, 王琦, 颜云松, 等. 计及网络攻击影响的安全稳定控制系统风险评估方法[J]. 电力工程技术, 2022, 41(3): 14-21.
[16] 姚登凯, 王晴昊, 甘旭升. 改进模糊Petri网在空管安全风险评估中的应用[J]. 安全与环境学报, 2018, 18(2): 413-417.
[17] 陈伟伟, 吕盼, 纪凤坤, 等. 基于多维度检测与Petri网的变电站接地故障风险评估[J]. 电力系统保护与控制, 2019, 47(23): 152-160.
[18] 孟邹清. 第六十二讲: 数字化工厂风险评估案例浅析[J]. 仪器仪表标准化与计量, 2017(6): 14-16.

作者简介:

王佳（1986—），通信作者，男
级工程师。主要研究方向：智能
成熟度评估。
E-mail: wangjia@cstc.org.

赵文苹（1989—），女，河北保
要研究方向：数字化转型能力研
E-mail: zhaowenping@cstc.

秦嘉言（1992—），女，河北保
研究方向：智能制造软件产品测
E-mail: qinjiayan@cstc.or

工业技
Industrial Techn
2022年
(Gongye Jish
主管单位：中华人民
主办单位：中国电子
赛迪工业
出版单位：北京赛迪
主　　编：张　阔
责任编辑：吕红秋
美术编辑：吴　桐
编辑电话：010-8855
发行单位：北京赛迪出
订阅热线：010-8855
传　　真：010-88558
主　　页：gyjs.cbpt
邮　　箱：gyjscx@c
出版日期：2022年10月
广告发布登记：京海工
承　　印：廊坊市鸿煊
编辑出版地址：北京市

Risk Assessment Model for Intelligent Factory Assets Using Object-Oriented Petri Net and Its Application Study

WANG Jia, ZHAO Wenping, QIN Jiayan
(*China Software Testing Center, Beijing 100048, China*)

Abstract: Risk assessment is an effective strategy to identify the risks of assets in the intelligent factories and ensure the safe operation of assets in the digital manufacturing enterprises. Focusing on the factors including asset value, threat and vulnerability in the asset system structure of intelligent factory, the assessment strategy of asset value and asset security risk value was put forward. The Ordered Weighted Geometric Average (OWGA) operator was used to effectively gather data information and sort the importance of assets, so that the security risks could be sorted by calculating the weights of assets, risk probability and threat consequences, and further to improve the objectivity and measurability of risk assessment of assets. By considering the information transfer between assets and the analysis of security characteristics, the risk assessment process was formed. The Petri net topological structure of asset identification, threat identification and security policy identification was established by adopting the 4 kinds of relationship forms of mutual influence of assets called sequential, common, concurrent and secondary. An example shows that such a model can guide the complex systems such as intelligent factories to design corresponding security protection measures by using the parametric characteristics of asset importance, risk probability, threat consequences, etc., so as to ensure a high management, operation and maintenance level of assets.

Keywords: Intelligent Factory; Risk Assessment; Petri Net; Ordered Weighted Geometric Average (OWGA); Complex System

工业技术创新
Industrial Technology Innovation
（双月刊）

目次

第9卷 第5期 2022年10月 总第52期

专题：智造技术

高炉炉热闭环智能控制系统研究与应用评价 …… 王军，郑伟，李泽安，王德智，王晓雪，赵宏博 (001)

基于机器视觉的五金行业自动化组装生产线系统研究 …… 刘鹏，刘凤义 (011)

面向对象的Petri网智能工厂资产风险评估模型及应用研究 …… 王佳，赵文苹，秦嘉言 (019)

智能造球理论方法及应用研究 …… 刘原，黄俊昱，赵宏博，张力，徐继伟 (028)

专题：新材料

沸石—地聚合物复合多孔材料制备及其二氧化碳吸附性能研究 …… 李娟，吴虎 (040)

以Mo/Al/B_2O_3/金刚石粉体热爆反应体系在金刚石颗粒表面形成镀覆涂层 …… 史冬丽，马尧，李涛，梁宝岩 (047)

铝合金硬质阳极氧化提高15-5PH不锈钢表面性能 …… 杜全强 (053)

单层粉和双层粉弹性金属塑料瓦的研究与比选 …… 杨优军，巴金，牛喜文 (059)

钻石及其相似品的鉴别研究 …… 辛虹瑾，姚泽，叶鹏，盛志远，罗艳梅，秦毅 (066)

专题：装备研制

高速铁路接触网定位钩和定位支座异常磨损分析 …… 王培 (073)

基于FPGA的高精度短时间间隔测量系统 …… 李恩丞，黄明，周元翰，张镇，李兴鑫 (081)