工业控制系统安全一体化风险评估方法

王红敏[1]，韩少云[2]，魏强[1]，宋思静[1]
（1. 信息工程大学，河南 郑州 450001；2. 河南工程学院，河南 郑州 450001）

摘　要：工业控制系统（ICS, industrial control system）关乎国家关键基础设施的正常运行，随着系统开放度的增大，工业控制系统面临信息域和物理域的双重风险，过去只对功能安全或信息安全某一方面进行风险评估已不再适用，因此，提出了对工业控制系统安全一体化的风险评估方法。在安全一体化风险量化评估过程中，风险传播路径分析、风险传播路径可能性计算和安全风险损失值量化是影响评估准确性的关键要素。首先，该方法结合 Petri Net 与蝴蝶结模型（bow-tie）各自的优势，分析了信息安全风险传播路径、功能安全风险传播路径和风险跨域传播路径。然后，运用专家知识、三角模糊数和质心公式计算功能安全风险传播的可能性，并基于漏洞评分系统和修正函数计算信息安全风险传播的可能性。最后，基于质量因子的思想给出关键事件损失量化模型。通过定量评估关键事件的风险值，能进一步在化工厂仿真环境中验证所提方法的有效性。

关键词：工业控制系统；功能安全；信息安全；蝴蝶结模型；Petri Net；安全一体化风险评估
中图分类号：TN929.5
文献标志码：A
doi：10.11959/j.issn.2096−3750.2025.00412

An integrated risk assessment method for industrial control system security

WANG Hongmin[1], HAN Shaoyun[2], WEI Qiang[1], SONG Sijing[1]
1. Information Engineering University, Zhengzhou 450001, China
2. Henan University of Engineering, Zhengzhou 450001, China

Abstract: Industrial control system (ICS) is related to the normal operation of national key infrastructure. With the increase of system openness, industrial control systems are facing dual risks in the cyber domain and the physical domain. It was no longer applicable to only conduct risk assessment on one aspect of safety or security. A risk assessment method for the security integration of industrial control systems was proposed to address this. In the process of quantitative risk assessment for security integration, risk propagation path analysis, calculation of the likelihood of risk propagation paths, and quantification of the loss value of security risks are the key elements that affect the accuracy of the assessment. Firstly, the method combined the respective advantages of Petri Net and the bow-tie model to analyze both security risk propagation paths, safety risk propagation paths, and risk cross-domain propagation paths. Then, the expert knowledge, trigonometric fuzzy number and centroid formula was used to calculate the possibility of safety risk propagation, and the probability of information security risk propagation was calculated based on the vulnerability scoring system and correction function. Finally, based on the idea of mass factor, a quantitative model of key event loss was given. By quantitatively assessing the risk value of critical events, the effectiveness of the proposed methodology can be further validated in a chemical plant simulation environment.

Key words: industrial control system, safety, security, bow-tie, Petri Net, integrated security risk assessment

收稿日期：2024−09−19；**修回日期：**2024−10−27
通信作者：魏强，prof_weiqiang@163.com
基金项目：国家重点研发计划项目（No. 2020YFB2010902）
Foundation Item: The National Key Research and Development Program of China (No. 2020YFB2010902)

0 引言

国家关键基础设施关乎国计民生，80% 以上的国家关键基础设施由工业控制系统（ICS, industrial control system）实现自动化，随着工业化和信息化的深度融合，ICS 的封闭性被打破。近年来，针对 ICS 的网络攻击事件频繁发生，带来了巨大的经济、人员等损失，隔离即安全的时代已经成为历史，对 ICS 进行风险评估有助于降低安全事件带来的损失。由于 ICS 由信息域和物理域两部分构成[1]，信息域的风险可能传播到物理域，物理域的风险也可能传播到信息域，这导致其面临信息域和物理域的双重风险。因此，对系统只进行功能安全风险评估或信息安全风险评估已无法满足安全需要，亟须开展安全一体化风险评估[2]。

目前，对于安全一体化风险评估研究的成果较少，通过研究现有的成果发现，基于模型的安全风险评估方法使用较为广泛，它能完备地分析风险传播路径并精确地计算安全事件发生的概率，是当前的主要研究方向。文献[3]将蝴蝶结模型与攻击树相结合，该方法通过蝴蝶结模型刻画功能安全风险传播路径，使用攻击树模型刻画信息安全风险传播路径，但是该方法使用定性量表的方法分别分析信息安全风险传播的可能性和功能安全风险传播的可能性，具有一定的主观性，难以量化，且结果不稳定。文献[4]运用贝叶斯网络评估网络攻击对物理域的影响，该方法最终构建的模型是包含脆弱性节点、特权节点和目标节点的层次结构，通过该方法从控制论的角度推断传感器和执行器被破坏的概率及安全事件带来的损失，但该方法未细致地刻画风险传播路径及安全事件损失所涵盖的具体方面。文献[5]同样基于贝叶斯网络来定量评估网络攻击对分布式信息物理系统带来的风险，在计算风险传播的可能性时包括先验概率和后验概率两部分，其中，先验概率通过信息熵计算基本事件发生的可能性，后验概率通过传染病模型计算前置节点传播到后置节点的风险概率值，该方法比较细致地计算了风险传播可能性，并通过最小负载损失计算虚假数据注入和修改断路器开关这两种威胁模式的负载损失比，但该方法未说明如何刻画不同的风险传播路径，且该安全事件损失值的计算方法并不适用于其他行业，不具有普适性。文献[6]考虑了信息域风险至物理域的传播，提出了一种包含攻击、功能和事件的多级贝叶斯网络模型，能够动态地评估网络风险。第二年，该团队又设计了一种包含网络攻击、系统功能、危害事件和系统资产 4 个方面的模糊概率贝叶斯网络模型，通过专家知识获得条件概率表（CPT, conditional probability table)[7]。但这两种模型都只考虑了网络攻击带来的风险，没有考虑功能安全风险。由于 ICS 的 ATT&CK（adversarial tactics, techniques, and common knowledge）模型是针对工业控制系统实施攻击的战技术统一框架，包括初始进入、执行、持续、权限提升、隐蔽、发现、横向移动、收集信息、命令及控制、抑制响应、破坏控制过程和影响 12 个阶段，该框架详细地描述了每个阶段所包含的战术方法及对应的风险缓解措施，因此，近年来，基于 ATT&CK 模型对系统进行信息安全风险评估的研究成果逐步增加[8-9]，文献[10]针对社会工程学进行了风险评估的研究，但这些成果也只是对信息安全风险进行评估。此外，病毒传播、控制的研究成果也可为安全一体化风险传播提供思路[11-13]。

通过对上述不同模型的分析，本文分析研判总结安全一体化风险评估的关键点，并基于 Petri Net 和蝴蝶结模型各自的优势，提出了新模型（PN-BT, Petri Net-bow-tie），该模型用于量化评估 ICS 安全一体化风险。该模型具有如下 4 点优势：1) 在分析研判功能安全风险和信息安全风险的基础上，定义了安全一体化风险，并以图示化的方式描述了信息域风险至物理域的传播过程；2) 该模型能够识别并刻画导致某一安全事件的所有风险传播路径，包括功能安全风险传播路径、信息安全风险传播路径和信息安全功能安全风险传播路径 3 类；3) 以定量的方式计算风险传播路径发生的可能性，与现有方法相比，能够降低主观性并提高精确性；4) 以普适性的方式从人员损失、经济损失和环境影响 3 个维度计算安全事件带来的损失。

1 基本知识

1.1 Petri Net 基本知识

信息安全风险评估是计算安全事件带来的损失与安全事件发生可能性的乘积，但是由于安全事件造成的损失是确定值，因此信息安全风险评估的实质是计算安全事件发生的概率。一般而言，对于同

一个安全事件可能有多条攻击链路，且攻击链条具有异步、离散和并发的特性。鉴于Petri Net对于描述异步、离散和并发的系统很有优势[14-17]，因此，Petri Net较适用于信息安全风险评估。基本Petri Net主要由库所P、变迁T和流关系F组成，基本Petri Net模型如图1所示。库所P表示资产的脆弱性，变迁T表示脆弱性对应的威胁，流关系F连接库所与变迁，风险通过资产脆弱性的关联关系传播，传播方向通过库所与变迁之间的流关系表示。有时为了描述系统的当前状态，将标识M引入基本Petri Net。Petri Net是一个层次模型，不同的层次有不同的含义，它能够以图示化的方式描绘基于知识的推理过程，被越来越多地用于系统安全、可靠性和风险评估[14]。目前，以基本Petri Net为基础，衍生出多种Petri Net，比如贝叶斯Petri Net、模糊Petri Net等。Petri Net可以清晰地表示系统中存在的威胁、脆弱性和资产价值之间的关系，对应信息安全风险评估的三要素。具有连接关系的库所存在因果关系，通过概率公式计算库所值。

1.2　蝴蝶结模型基础知识

蝴蝶结（BT, bow-tie）模型是一种在系统功能安全风险评估中常用且有效的方法[18]，它最开始用于对整个安全事件场景的描述，后续用于风险管理、风险分析、风险评估和功能安全故障分析等方面的研究[19]。BT模型能够描述系统中不同风险控制参数之间的关系，能够推理和归纳事件产生的原因和后果。它由故障树和事件树两部分构成。故障树以图形化的方式刻画意外事件与基本原因之间的关系，在故障树中，它们分别表示为顶事件（TE, top event）和基本事件（BE, basic event）；事件树是事件产生后果的图模型，它将意外事件作为启动事件（IE, initator event），构建成功或失败的后果二叉树，生成的结果事件（OE, outcome event）为最终状态[19-20]。蝴蝶结模型将故障树的顶事件和事件树的启动事件作为关键事件（CE, critical event），事件与原因之间的关系通过与、或门连接。蝴蝶结模型如图2所示，其中，IE节点为中间事件。

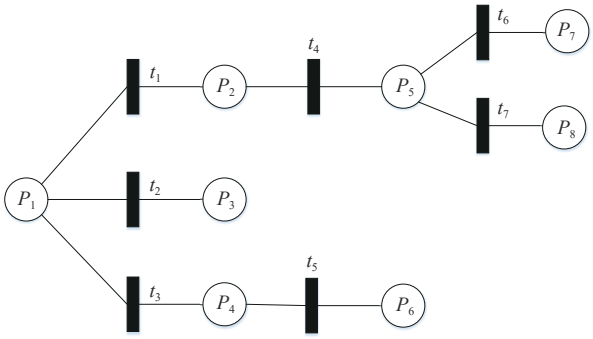

图1　基本Petri Net模型

2　相关研究

2.1　功能安全风险评估与信息安全风险评估的异同点

不论是功能安全风险评估还是信息安全风险评

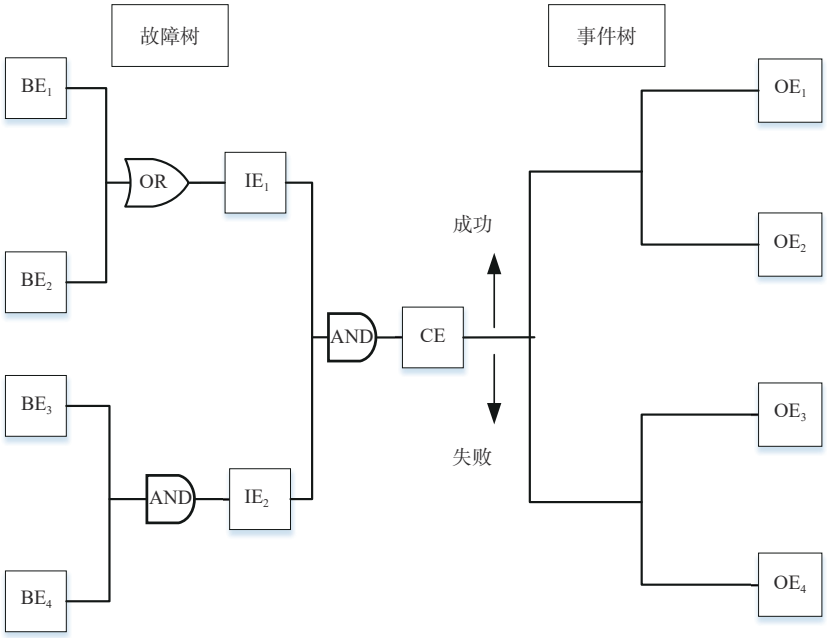

图2　蝴蝶结模型

估，本质都是计算安全事件发生的可能性及其造成后果的乘积。但是它们在风险来源、风险评估对象等方面存在很多不同之处，功能安全风险评估与信息安全风险评估的异同点见表 1。功能安全风险主要来源于系统设备故障或人员操作失误[21-23]；信息安全风险主要来源于内外部恶意人员利用系统脆弱性带来的风险[22-23]。功能安全风险发生的概率是计算某些事件发生的概率；而信息安全风险发生的概率是威胁利用资产脆弱点的可能性，具有不确定性。相比之下，信息安全风险发生的概率高于功能安全风险，功能安全事件是高影响低概率事件。由于功能安全风险评估与信息安全风险评估的本质不同，可能性的分析方法也不同。

2.2　安全一体化风险定义

工业控制系统涉及功能安全风险和信息安全风险[22-23]，在理论和实践中它们分别属于不同的学科，为了对安全一体化风险评估进行研究，需要对安全一体化风险这一概念进行定义。功能安全风险被定义为一系列不希望发生的事件及它的可能性和后果，即 $R_{\mathrm{sa}}=\{S_{e_i},P_{e_i},X_{e_i}\}$，$i=1,2,3,\cdots,N$[3]；信息安全风险被定义为威胁利用资产脆弱性的可能性及后果，即 $R_{\mathrm{se}}=\{(\mathrm{tv})_j,P_{(\mathrm{tv})_j},X_{(\mathrm{tv})_j}\}$，$j=1,2,3,\cdots,M$[3]。无论是功能安全风险还是信息安全风险，风险值的大小都通过风险发生的可能性和风险带来的损失这两个指标来衡量。

由于信息安全事件可能导致功能安全事件造成安全事件产生，因此，安全一体化风险被定义为一个 3 元组，如式(1)所示。其中，$S_{(\mathrm{tv},e,e_{-\mathrm{tv}})}$ 表示导致某一种安全事件 i 产生的风险传播路径集合，系统中可能存在多条导致该安全事件产生的路径。它可能由于威胁利用系统漏洞触发，即信息安全风险传播路径 tv；它也可能由功能安全事件触发，即功能安全风险传播路径 e；它还可能由信息安全导致功能安全事件最终触发该安全事件，即信息安全功能安全风险传播路径 $e_{-\mathrm{tv}}$；$P(\mathrm{tv},e,e_{-\mathrm{tv}})$ 风险传播路径发生的可能性，共包含信息安全风险传播路径 tv、功能安全风险传播路径 e 和信息安全功能安全风险传播路径 $e_{-\mathrm{tv}}$ 这 3 类路径发生的可能性；$X_{(\mathrm{hl},\mathrm{el},\mathrm{ei})_i}$ 表示安全事件 i 造成的损失，包括人员损失 hl、经济损失 el、环境影响 ei。

$$R=\{S_{(\mathrm{tv},e,e_{-\mathrm{tv}})_i},P(\mathrm{tv},e,e_{-\mathrm{tv}})_i,X_{(\mathrm{hl},\mathrm{el},\mathrm{ei})_i}\},\quad i=1,2,3,\cdots,N \tag{1}$$

为了更好地描述风险传播路径，将安全一体化风险以图示法表示，安全一体化风险定义如图 3 所示。功能安全风险传播路径通过 BT 刻画，其中 E 表示安全事件，DF 表示危险现象。信息安全风险传播路径通过 PN 刻画，其中 V 表示脆弱性，T 表示威胁。而信息安全功能安全风险传播路径通过 PN 与 BT 相连接共同刻画，威胁利用系统漏洞通过 PN 刻画，其达成的目标作为中间事件连接到 BT，如图 3 中的最低框图所示，信息域的风险沿着此路径传播至物理域。

3　安全一体化风险评估模型

安全一体化风险评估原理如图 4 所示。首先，由于安全一体化风险评估需要对风险要素进行识别，经研究发现，安全一体化风险评估的主要风险要素包括功能安全风险要素和信息安全风险要素两部分，其中，信息安全主要风险要素为资产、威胁和脆弱性，功能安全主要风险要素为资产、设备失效和操作失误。接着，计算安全事件发生的可能性，安全事件可能由信息安全事件导致，也可能由功能安全事件导致，还可能由信息安全事件触发功能安全事件导致，因此，需要考虑造成安全事件产生的所有可能路径。最后，计算安全事件发生的可能性与安全事件造成损失的乘积，即安全事件风险值。

表 1　　**功能安全风险评估与信息安全风险评估的异同点**

属性	功能安全风险评估	信息安全风险评估
评估对象	设备	区域、管道
风险属性	可能性、完整性、实时性	机密性、完整性、可用性
风险来源	设备故障、人员误操作、非故意性的危害	有意图攻击
风险发生概率	较低	较高
可能性计算相关因素	设备故障频率、操作人员技术水平	脆弱性等级、防护措施、技术难度
风险产生后的影响范围	系统本身或系统环境	系统环境

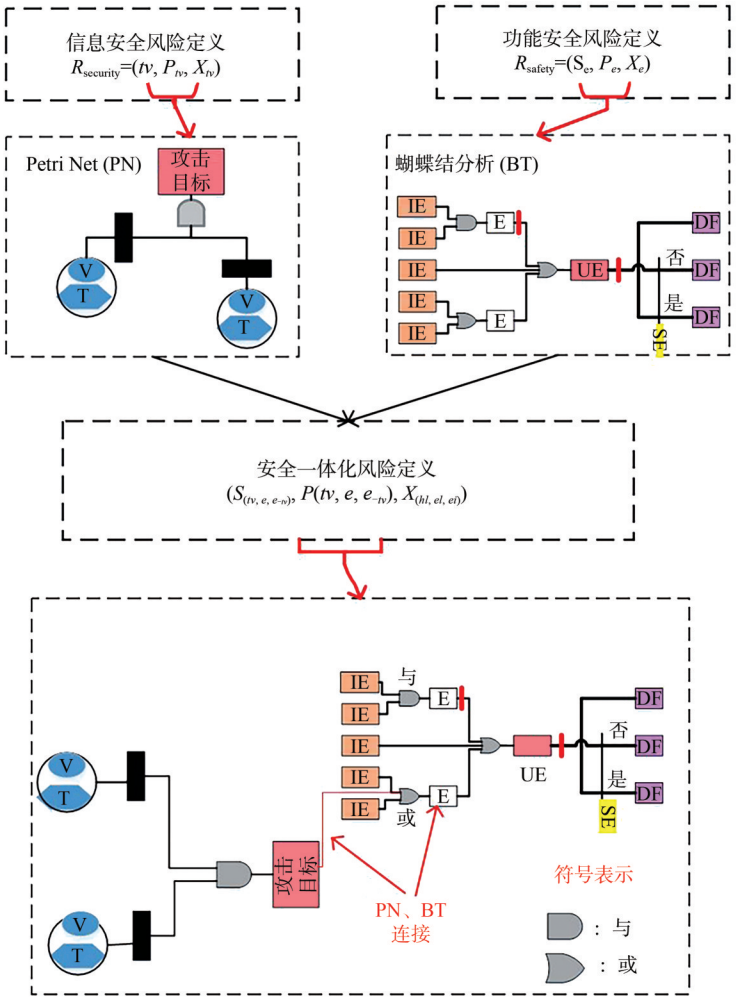

图3　安全一体化风险定义

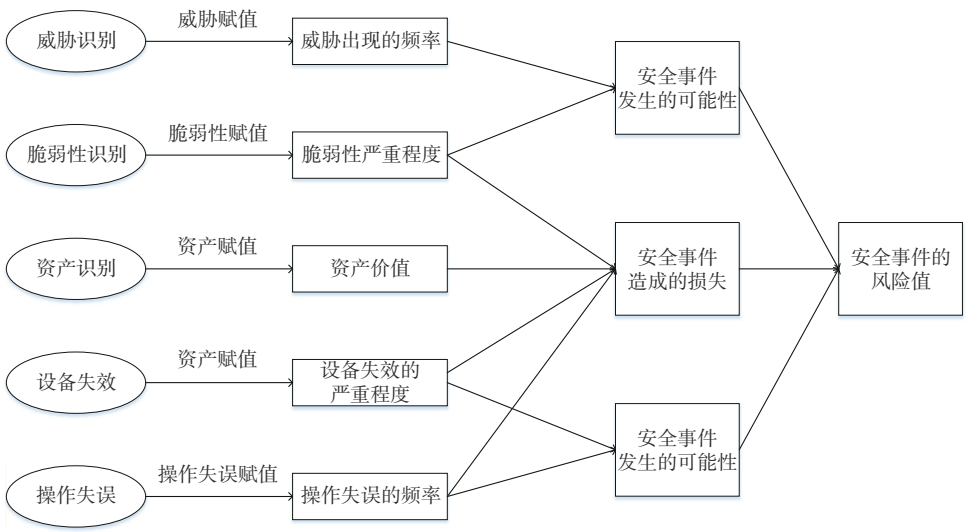

图4　安全一体化风险评估原理

本节介绍所提的安全一体化风险评估模型，该模型充分结合了Petri Net和蝴蝶结模型各自的优势，简称PN-BT。首先，通过Petri Net模型刻画信息安全风险传播路径、运用蝴蝶结模型刻画功能安全风险传播路径和Petri Net模型作为蝴蝶结模型的输入节点刻画信息安全功能安全风险传播路径；然

后，运用专家知识、三角模糊数和质心公式计算功能安全风险传播的可能性，运用漏洞评分系统、修正函数计算信息安全风险传播的可能性；最后，基于质量因子的思想从人员损失、经济损失和环境影响3个维度计算安全事件损失值。该模型能够充分刻画导致安全事件产生的风险传播路径并准确计算每条路径发生的可能性，结合安全事件造成的损失，最终准确地计算安全事件产生的风险值。接下来对风险传播路径、风险传播路径可能性计算和安全事件损失值计算这3个关键点依次展开分析。

3.1 安全事件风险传播路径分析

工业控制系统信息域与物理域高度耦合，风险既能够在信息域和物理域分别传播，也能够在信息域与物理域之间跨域传播。也就是说，信息域的风险可能传播到物理域，物理域的风险也可能传播到信息域。根据信息层、控制层和物理层各层级的功能及特性，本节将安全事件风险传播路径分为信息安全风险传播路径分析、功能安全风险传播路径分析和信息安全功能安全风险跨域传播路径分析3个方面，并分别展开研究。

3.1.1 信息安全风险传播路径分析

信息安全风险传播路径通过Petri Net模型构建，由于对信息层攻击者通常采用的策略是通过漏洞扫描、漏洞挖掘等方式找到脆弱性较大的资产，然后根据资产之间的信任关系利用资产脆弱性最终到达目标节点。因此，为了分析信息安全风险传播路径应首先分析系统的网络拓扑结构，然后深入挖掘资产节点间的信任关系、资产漏洞与风险传播路径的内在逻辑，找到影响信息层风险传播路径的关键因素。研究发现，信息层风险传播路径以遭受内外部威胁的节点作为基本节点，可能被波及的节点作为生成节点，依次利用资产脆弱性推至目标节点，最终形成整个风险传播路径。整个信息安全风险传播路径链条是威胁利用资产的脆弱性形成的，在利用Petri Net刻画信息安全风险传播路径的过程中，脆弱性及其对应的威胁用库所表示，该组合表示法能够使研究人员更直观地观察到系统脆弱性及其对应的威胁，威胁利用脆弱性达到的效果用变迁表示，库所之间具有顺序逻辑、逻辑与和逻辑或3种推理关系，改进的Petri Net推理模型如图5所示。其中，顺序逻辑表示P_1与P_2之间是先后关系；逻辑与表示只有当P_1与P_2同时发生时，P_3才发生；逻辑或表示只要P_1与P_2有一个发生，P_3就发生。

3.1.2 功能安全风险传播路径分析

相比于信息安全风险，功能安全风险发生的可能性较小。功能安全风险传播路径与物理层有关，物理层风险来源主要有以下3类：1) 设备故障；2) 人员误操作；3) 非故意性危害。功能安全风险传播路径通过蝴蝶结模型刻画，人员误操作、设备故障和非故意性危害表示为模型中的基本事件，通过研究发现，被控制器控制的物理层可建模为变量离散时间线性时变系统，如式(2)所示[4]，其中，x_k表示系统状态，u_k表示控制器状态，y_k表示传感器读数，$\boldsymbol{A}$、$\boldsymbol{B}$和$\boldsymbol{C}$表示物理层的动力学矩阵，w_k和v_k为零均值高斯噪声。式(2)说明了物理层系统组件之间的依赖关系，风险可根据物理层拓扑结构在设备之间级联传播，单个设备内具有多个参数，且参数之间具有关联性，根据物理生产工艺流程等，设备内某个参数的变化会影响其他参数，风险可在单个设备之间传播。风险根据组件之间的依赖关系传播导致中间事件的产生，然后中间事件之间的逻辑关系最终导致顶事件的产生。

$$\begin{cases} x_{k+1} = \boldsymbol{A}x_k + \boldsymbol{B}u_k + w_k \\ y_k = \boldsymbol{C}x_k + v_k \end{cases} \tag{2}$$

3.1.3 信息安全功能安全风险跨域传播路径分析

信息层设备通过调节控制层设备的控制参数来间接控制物理设备。根据工业控制系统的特点和控制层的功能，风险有多种跨域传播方式。风险跨越传播通常是由网络攻击导致的，通常可分为3种：1) 攻击者篡改信息层与控制层间的通信；2) 攻击

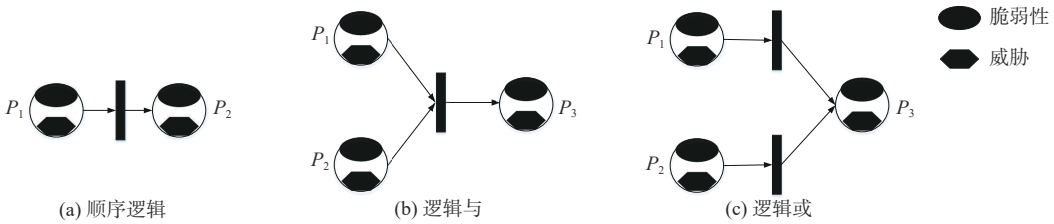

图5　改进的Petri Net推理模型

者篡改传感器信息；3) 攻击者篡改控制器与执行器间的通信。以上3种情况均可导致风险跨域传播，最终导致控制层向物理层下发错误的控制指令，影响物理层的正常运行。探究控制层的控制逻辑，分析系统遭受攻击后的动态变化等对于研究风险在信息层与物理层之间的传播路径至关重要。控制层由控制回路构成，通常采用比例积分微分（PID, proportional-integral-derivative）控制算法控制整个回路，理想的PID控制算法如式(3)所示。攻击者通过修改控制算法的参数来控制物理层设备。通过上述描述可知，一些情况下，信息安全事件能够导致功能安全事件的产生，此种情况需通过Petri Net和蝴蝶结模型共同刻画。因为它是由网络攻击事件引发，所以通过库所描述威胁利用资产脆弱性过程，产生的后果作为蝴蝶结模型的基本事件。

$$u(t) = K_p(e(t) + \frac{1}{T_1}\int_0^t e(t)\mathrm{d}t + T_D\frac{\mathrm{d}e(t)}{\mathrm{d}t}) \quad (3)$$

3.2　可能性计算

在找到风险传播路径后，接下来计算每条路径发生的可能性，文献[3]已经解释了分别计算功能安全风险传播路径和信息安全风险传播路径的必要性，这里不再赘述。因此，风险传播路径包括导致安全事件发生的功能安全风险传播路径、信息安全风险传播路径和信息安全功能安全风险跨域传播路径3个部分。通过计算每条路径发生的可能性并排序，能够找出风险值最大的路径，即安全事件的风险值。然后分析该路径产生的原因，找出系统的薄弱环节，给出相应的安全措施，提高系统的防护能力。

3.2.1　功能安全风险传播路径可能性计算

物理层的风险来源较广，如自然环境、设备失效、操作失误等。风险传播路径可能性计算的目的是计算物理层设备失效、操作失误等风险因素的概率。由于缺乏精确的数据和概率密度函数，功能安全风险传播路径基本事件发生可能性一般通过专家经验、知识获得，如非常高、高、底、非常低等主观观点[24]，专家知识对于基本事件发生可能性的判定具有主观性、模糊性、不确定性等特点。而模糊集理论能够处理专家经验的模糊性和主观性带来的不确定性，又由于三角模糊数（TFN, triangular fuzzy number）较适用于风险评估领域，因此，本文使用TFN将专家观点定量为区间概率。一个TFN由一个向量$(P_{\mathrm{L}}, P_{\mathrm{M}}, P_{\mathrm{U}})$表示，它们分别表示事件发生的最小概率、最可能的概率和最大概率，当前通常使用八语言变量[10]描述基本事件发生的可能性，语言等级的模糊等级如图6所示[20]。

然后运用质心公式[24-25]去模糊化。对于TFN，$D_1 = (P_{\mathrm{L}}, P_{\mathrm{M}}, P_{\mathrm{U}})$，转化后的质心公式如式(4)所示，其中，$X$为去模糊化后的结果，$x$为论域内概率取值。

$$X = \frac{\int_{P_{\mathrm{L}}}^{P_{\mathrm{M}}} \frac{x - P_{\mathrm{L}}}{P_{\mathrm{M}} - P_{\mathrm{L}}} x\mathrm{d}x + \int_{P_{\mathrm{M}}}^{P_{\mathrm{U}}} \frac{P_{\mathrm{U}} - x}{P_{\mathrm{U}} - P_{\mathrm{M}}} x\mathrm{d}x}{\int_{P_{\mathrm{L}}}^{P_{\mathrm{M}}} \frac{x - P_{\mathrm{L}}}{P_{\mathrm{M}} - P_{\mathrm{L}}} \mathrm{d}x + \int_{P_{\mathrm{M}}}^{P_{\mathrm{U}}} \frac{P_{\mathrm{U}} - x}{P_{\mathrm{U}} - P_{\mathrm{M}}} \mathrm{d}x} = \frac{P_{\mathrm{U}}^2 - P_{\mathrm{L}}^2 + P_{\mathrm{U}}P_{\mathrm{M}} - P_{\mathrm{L}}P_{\mathrm{M}}}{3(P_{\mathrm{U}} - P_{\mathrm{L}})} \quad (4)$$

由于专家背景知识不同，他们对同一事件发生可能性的评价也不同，因此需要对专家观点聚合，最终对基本事件发生的可能性达成一致观点。

3.2.2　信息安全风险传播路径可能性计算

信息侧风险主要通过系统设备、协议、工业软件等脆弱性传播，风险传播可能性大小与脆弱性等级密切相关，因此，识别脆弱性对于信息侧风险评估至关重要。通过查阅文献发现，脆弱性被利用的可能性主要通过通用漏洞评分系统（CVSS, common vulnerability scoring system）[26]计算，CVSS主要有3组评估指标：基准类指标、时间类指标和环

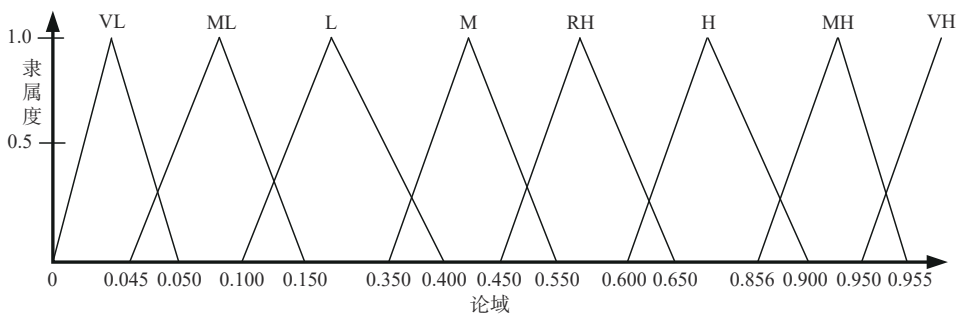

图6　语言等级的模糊等级

境类指标。脆弱性被利用的严重程度主要与基准类指标相关，之后运用文献[22]中的表 2 对基准类指标进行量化，最终脆弱性被利用的计算如式(5)所示[22, 27]。然而，对于 CVSS 2.0 中的脆弱性信息通过式(6)计算[4]。

$$p = \frac{8.22 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{PR} \times \mathrm{UI}}{10} \tag{5}$$

$$p = \mathrm{S\_AV} \times \mathrm{S\_AC} \times \mathrm{S\_AU} \tag{6}$$

无论是信息安全风险传播路径还是功能安全风险传播路径，都是通过逻辑与、或门将基本事件相连构建顶事件。其中，逻辑与门表示只有当所有基本事件发生时，顶事件才发生。假如对于顶事件有 m 个基本事件，且各个基本事件相互独立，当 m 个基本事件都发生时，顶事件才发生，通过式(7)计算通过与门构造的顶事件发生概率。当其中一个基本事件发生时，顶事件就发生，对于此类情况通过逻辑或门表示，通过或门构建的顶事件发生的概率用式(8)计算。式(7)和式(8)中，$Q(t)$表示顶事件发生的概率，$Q_b(t)$表示基本事件发生的概率。

$$Q(t) = \prod_{b=1}^{m} Q_b(t), b = 1, 2, 3, \cdots, m \tag{7}$$

$$Q(t) = 1 - \prod_{b=1}^{m} (1 - Q_b(t)), b = 1, 2, 3, \cdots, m \tag{8}$$

3.3　安全事件损失值计算

本节分析安全事件发生后带来的损失，进一步量化风险值。为了更好地量化安全事件带来的损失 Lv，本节主要从人员损失、经济损失和环境影响 3 个关键因素对损失值进行量化，关键事件损失量化模型如图 7 所示。

hl 为人员损失，按照人员损失的严重程度划分为 1、2 和 3 这 3 个等级；el 为经济损失，按照经济损失的严重程度划分为 1、2 和 3 这 3 个等级；ei 为环境影响，按照环境影响程度划分为 1、2 和 3 这 3 个等级。模型的这 3 个关键因素为损失值计算的关键指标，计算如式(9)所示，损失值定义为各指标连线所包围的面积之和。

$$\begin{cases} \mathrm{Lv} = \sum_{i=1}^{3} S_i \\ S_1 = \frac{1}{2}\mathrm{ei} \times \mathrm{hl} \\ S_2 = \frac{1}{2}\mathrm{ei} \times \mathrm{el} \\ S_3 = \frac{1}{2}\mathrm{el} \times \mathrm{hl} \end{cases} \tag{9}$$

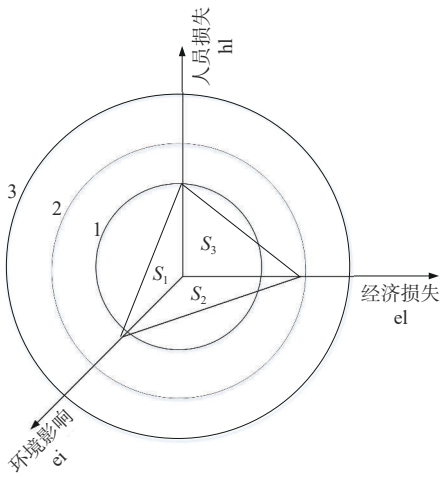

图 7　关键事件损失量化模型

4　实验与结果

4.1　实验环境

本节主要对第 3 节提出的安全一体化风险评估模型进行验证，旨在验证该模型的可行性和有效性。它适用于任何行业，本节以该模型在工业控制系统安全模拟的图形化框架（GRFICS, graphical realism framework for industrial control simulation）中应用为例进行验证[28-29]。GRFICS 由 Fortiphyd 研究所和美国佐治亚理工学院的研究人员开发，GRFICS 功能结构如图 8 所示。图 8 中 scada 为工程师站、pfSense 为防火墙、PLC 为控制器、ChemicalPlant 为物理过程仿真环境、Workstation 为 PLC 的工作环境、Kali 为攻击机，Kali 与工程师站在同一网段，这些组件通过标准的 ICS 网络协议连接，人机界面（HMI, human machine interface）显示现场各参数值，可编程逻辑控制器（PLC, programmable logic controller）控制现场物理过程。

图 8 中物理过程仿真环境是化工厂模型平台，是简化的田纳西—伊斯曼（TE，Tennessee Eastman）仿真环境，包括反应和分离两个阶段，共具有 8 个状态、4 个操纵控制阀门和 10 个输出测量值。其中，GRFICS 管道仪表如图 9 所示，包括传感器、执行器和控制器，该平台中的执行器为阀门。

反应器内的化学反应如式(10)所示[29-30]，气体 A、B 在催化剂 B 的作用下生成液体 D，图 9 各符号名称见表 2。反应器在稳定状态下，产品 D 的生产率为 100 kmol/h，压力值 P 为 2 700 KPa，Purge 中 A 的含量为 47 mol%。通过 4 个控制回路使反应器内

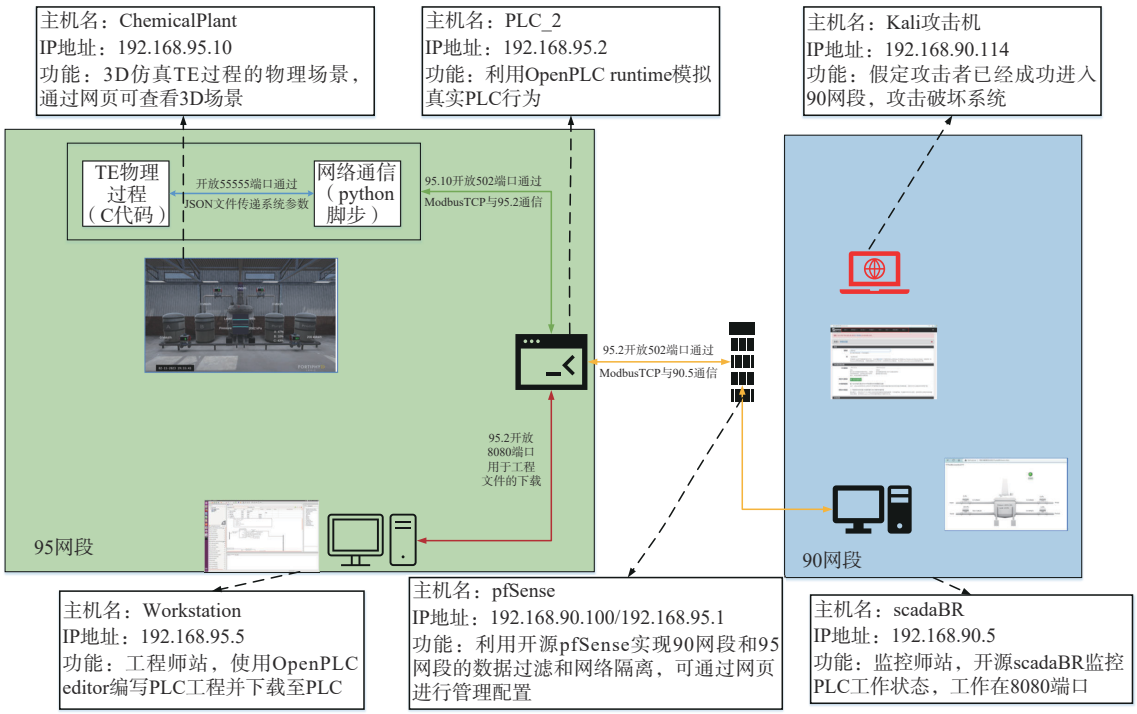

图8　GRFICS功能结构

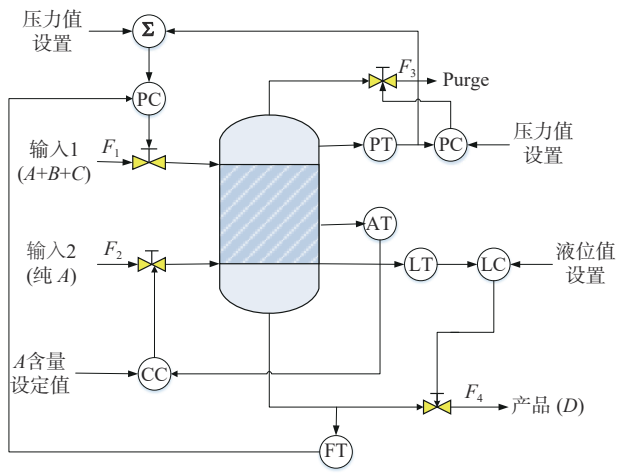

图9　GRFICS管道仪表

表2　　图9各符号名称

符号	名称	符号	名称
	阀门	PT	压力传感器
PC	压力控制器	AT	反应器内气体A含量传感器
LT	液位传感器	LC	液位控制器
FT	流量传感器	CC	反应器内气体A含量控制器

的关键指标处于稳定状态：1) 反应器内压力值控制方式较多，一方面，PC通过PT的值和压力设置值控制反应器内的压力值，另一方面PC通过FT值、PT值及压力设置值操作F_1控制反应器压力值；2) LC通过LT的测量值与液位设置值控制F_4操纵F_4的开度使反应器液位达到稳定状态；3) CC通过AT的测量值与A含量设置值控制F_2的开度使Purge中A的含量达到稳定状态。

$$A + C \xrightarrow{B} D \tag{10}$$

4.2　风险传播路径构建

对于化工厂，压力值异常是一个严重问题，一旦发生将产生爆炸或者化学反应停止，造成严重的经济损失。因此，将压力值异常作为一个安全事件，本节主要分析压力值超过3 200 KPa发生爆炸此种情况。一般情况下，可通过信息安全事件和功能安全事件导致压力值超过3 200 KPa。信息安全事件主要由网络攻击引起，功能安全事件主要由设备故障、人员误操作等因素导致。在信息侧并不是所有的攻击都能使压力值超过3 200 KPa，通过实验研究及理论分析发现，可通过ARP攻击、注入恶意Modbus命令攻击、控制逻辑篡改、获取scadaBR shell权限、获取pfSense shell权限这5种方式导致现场层反应器内压力值异常。在物理侧，通过研究管道仪表图[13]发现，基于专家知识主要通过化学反应异常、阀门开度异常和压力表故障这3种方

式导致现场层反应器内压力值异常，但它们发生的概率较低。综合考虑分析导致压力值异常功能安全事件和信息安全事件，GRFICS 的 PN-BT 模型如图 10 所示。

由于信息安全事件造成反应器内压力值超过 3 200 KPa，发生爆炸的风险传播路径共有 7 条，分别为：第 1 条风险传播路径 L_{e1} 为利用 scadaBR CVE-2021-26828 漏洞获取 scadaBR Tomcat 权限删除关键

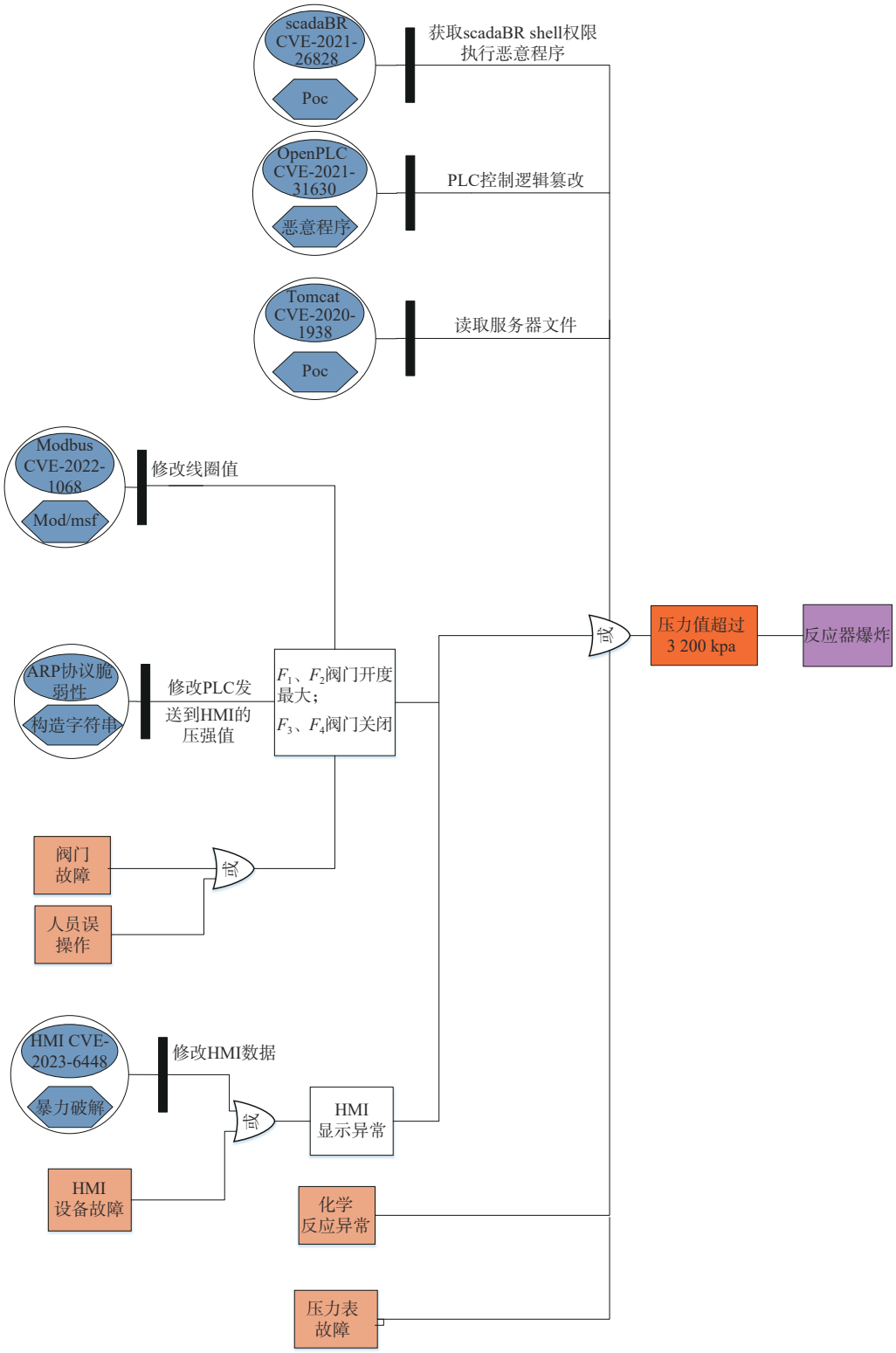

图 10　GRFICS 的 PN-BT 模型

数据信息；第2条风险传播路径L_{e2}为通过OpenPLC Web界面上传恶意程序修改PLC的控制逻辑；第3条风险传播路径L_{e3}为利用scadaBR Tomcat CVE-2020-1938漏洞获得scadaBR权限删除关键信息；第4条风险传播路径L_{e4}为利用Modbus CVE-2022-1068脆弱性修改线圈值使阀门F_1和F_2开度最大，阀门F_3和F_4关闭；第5条风险传播路径L_{e5}为利用ARP协议脆弱性构造字符串修改PLC发送到HMI的压强值；第6条风险传播路径L_{e6}为利用HMI弱口令的脆弱性修改HMI显示的压力值；第7条通过人员误操作、压力表故障、HMI故障、阀门故障和化学反应异常这5种功能安全事件导致压力值超过3 200 KPa，从而关键事件产生。

4.3　风险传播路径可能性计算

由于安全事件为反应器发生爆炸，无论是由于信息安全事件触发还是功能安全事件触发，爆炸发生后带来的损失是相同的，因此接下来只需分析事件发生的可能性。

根据第3.2.1节功能安全风险传播路径可能性计算方法，分别计算设备故障、人员误操作和化学反应异常发生的可能性。通过调研领域专家，压力表故障发生的概率比较低，属于八语言变量的L等级，它的概率计算过程如式(11)所示。人员误操作属于八语言变量的VL等级，它的概率计算过程如式(12)所示。化学反应异常属于八语言变量的ML等级，它的概率计算过程如式(13)所示。

$$P_1=\frac{P_{\mathrm{U}}^2-P_{\mathrm{L}}^2+P_{\mathrm{U}}P_{\mathrm{M}}-P_{\mathrm{L}}P_{\mathrm{M}}}{3(P_{\mathrm{U}}-P_{\mathrm{L}})}=\frac{0.4^2-0.1^2+0.1-0.025}{3\times(0.4-0.1)}=0.25 \tag{11}$$

$$P_2=\frac{P_{\mathrm{U}}^2-P_{\mathrm{L}}^2+P_{\mathrm{U}}P_{\mathrm{M}}-P_{\mathrm{L}}P_{\mathrm{M}}}{3(P_{\mathrm{U}}-P_{\mathrm{L}})}=\frac{0.05^2+0.001\,25}{3\times0.05}=0.025 \tag{12}$$

$$P_3=\frac{P_{\mathrm{U}}^2-P_{\mathrm{L}}^2+P_{\mathrm{U}}P_{\mathrm{M}}-P_{\mathrm{L}}P_{\mathrm{M}}}{3(P_{\mathrm{U}}-P_{\mathrm{L}})}=\frac{0.15^2-0.045^2+0.014\,625-0.004\,387\,5}{3\times0.105}=0.097\,5 \tag{13}$$

通过对比上述计算结果，能够发现对于功能安全事件，设备故障发生的可能性比人员误操作和化学反应异常发生的可能性要高，因此，为了降低安全事件带来的损失，可通过经常检查设备等方式降低此类风险。

根据第3.2.2节信息安全风险传播路径可能性计算方法，分别计算L_{e1}、L_{e2}、L_{e3}、L_{e4}、L_{e5}发生的可能性。

对于L_{e1}，通过查找CVSS 3.0，CVE-2021-26828的攻击向量（AV, attack vector）为network、攻击复杂度（AC, attack complexity）为low、权限需求（PR, privilege required）为low、用户互动（UI，user interaction）为none，L_{e1}可能性的计算过程如式(14)所示。

$$P_4=\frac{8.22\times\mathrm{AV}\times\mathrm{AC}\times\mathrm{PR}\times\mathrm{UI}}{10}=\frac{8.22\times0.85\times0.77\times0.62\times0.85}{10}=0.28 \tag{14}$$

对于L_{e2}，该路径利用OpenPLC设备的CVE-2021-31630执行恶意程序。通过查找CVSS 3.0，CVE-2021-31630的AV为network、AC为low、PR为low、UI为none，L_{e2}可能性的计算过程如式(15)所示。

$$P_5=\frac{8.22\times\mathrm{AV}\times\mathrm{AC}\times\mathrm{PR}\times\mathrm{UI}}{10}=\frac{8.22\times0.85\times0.77\times0.62\times0.85}{10}=0.28 \tag{15}$$

对于L_{e3}，通过查找CVSS 3.0，CVE-2020-1938的AV为network、AC为low、PR为none、UI为none，L_{e3}可能性的计算过程如式(16)所示。

$$P_6=\frac{8.22\times\mathrm{AV}\times\mathrm{AC}\times\mathrm{PR}\times\mathrm{UI}}{10}=\frac{8.22\times0.85\times0.77\times0.85\times0.85}{10}=0.39 \tag{16}$$

对于L_{e4}，通过查找CVSS 3.0，CVE-2022-1068的AV为network、AC为low、PR为none、UI为none，L_{e4}可能性的计算过程如式(17)所示。

$$P_7=\frac{8.22\times\mathrm{AV}\times\mathrm{AC}\times\mathrm{PR}\times\mathrm{UI}}{10}=\frac{8.22\times0.85\times0.77\times0.85\times0.85}{10}=0.39 \tag{17}$$

对于L_{e5}，该路径利用ARP脆弱性，虽然没有ARP的CVE编号，但是经研究发现CVE-1999-0667与ARP攻击的原理类似。通过查找CVSS 2.0，CVE-1999-0667的AV为network、AC为low、PR为none，L_{e5}可能性的计算过程如式(18)所示。

$$P_8=2\times\mathrm{S\_AV}\times\mathrm{S\_AC}\times\mathrm{S\_AU}=2\times1\times0.71\times0.704=0.99 \tag{18}$$

对于HMI显示异常事件，存在两条路径：1) 利用CVE-2023-6448，即路径L_{e6}；2) HMI本身设备故障。对于L_{e6}，通过查找CVSS 3.0，CVE-2023-6448的

AV为network、AC为low、PR为none、UI为none，L_{e6}可能性的计算过程如式(19)所示，而HMI设备故障的概率是0.25，这也说明了对于同一安全事件，功能安全事件发生的可能性小于信息安全事件。

$$P_9 = \frac{8.22 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{PR} \times \mathrm{UI}}{10} = \frac{8.22 \times 0.85 \times 0.77 \times 0.85 \times 0.85}{10} = 0.39 \tag{19}$$

4.4 实验结果分析与对比

通过上述结果可以发现，功能安全风险发生的可能性低于信息安全风险，L_{e1}~L_{e6}这6条信息安全风险传播路径中，利用ARP协议缓冲区溢出脆弱性造成反应器发生爆炸的可能性最大，因此，应采取与ARP缓冲区溢出相对应的风险缓解措施，降低风险发生的概率。为了进一步验证本文所提的PN-BT模型的有效性，将该方法与传统的攻击树、故障树、蝴蝶结模型、Petri Net相比较。风险评估方法的比较见表3，通过比较发现PN-BT模型既能对信息域风险评估，又能对物理域风险评估，还能对跨域风险评估，而传统的方法只能进行单一类别的风险评估。

表3　　风险评估方法的比较

方法名称	信息域风险评估	物理域风险评估	信息域物理域风险评估
攻击树	是	否	否
故障树	否	是	否
蝴蝶结模型	否	是	否
Petri Net	是	否	否
PN-BT	是	是	是

5 结束语

工业控制系统的安全一体化问题关乎国家关键基础设施的正常运行，对其进行安全一体化风险评估至关重要。本文在进行一体化安全风险评估时，首先，在功能安全风险和信息安全基础上，定义安全一体化风险；然后，从功能安全风险传播路径、信息安全风险传播路径和信息安全功能安全风险传播路径3个方面分析风险传播路径模型；接着，运用质心公式、修正函数等方法计算风险传播路径发生的可能性，并从人员损失、经济损失和环境影响3个维度刻画安全事件损失值；最后，通过GRFICS场景验证所提模型的有效性。未来将研究风险传播机理，包括风险传播速度、风险的控制等，进一步提高工业控制系统的安全性。

参考文献：

[1] KRIAA S, PIETRE-CAMBACEDES L, BOUISSOU M, et al. A survey of approaches combining safety and security for industrial control systems[J]. Reliability Engineering & System Safety, 2015, 139: 156-178.

[2] Gaithersburg: National Institute of Standards and Technology (NIST). Guide to industrial control system (ICS) security: NIST SP800-82[S]. 2014.

[3] ABDO H, KAOUK M, FLAUS J M, et al. A safety/security risk analysis approach of industrial control systems: a cyber bowtie-combining new version of attack tree with bowtie analysis[J]. Computers & Security, 2018, 72: 175-195.

[4] HUANG K X, ZHOU C J, TIAN Y C, et al. Assessing the physical impact of cyberattacks on industrial cyber-physical systems[J]. IEEE Transactions on Industrial Electronics, 2018, 65(10): 8153-8162.

[5] DENG S, ZHANG J T, WU D, et al. A quantitative risk assessment model for distribution cyber-physical system under cyberattack[J]. IEEE Transactions on Industrial Informatics, 2023, 19(3): 2899-2908.

[6] ZHANG Q, ZHOU C J, XIONG N X, et al. Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016, 46(10): 1429-1444.

[7] ZHANG Q, ZHOU C J, TIAN Y C, et al. A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2018, 14(6): 2497-2506.

[8] AMRO A, GKIOULOS V, KATSIKAS S. Assessing cyber risk in cyber-physical systems using the ATT&CK framework[J]. ACM Transactions on Privacy and Security, 2023, 26(2): 1-33.

[9] WANG Y M, WANG W H, BAI X X, et al. RRDD: an ATT&CK-based ICS network security risk assessment method[C]//Proceedings of the 2023 2nd International Conference on Networks, Communications and Information Technology. New York: ACM Press, 2023: 186-192.

[10] LIU K X, XIE Y F, XIE S W, et al. SEAG: a novel dynamic security risk assessment method for industrial control systems with consideration of social engineering[J]. Journal of Process Control, 2023, 132: 103131.

[11] BI J C, YANG X F, WU Y B, et al. On the optimal dynamic control strategy of disruptive computer virus[J]. Discrete Dynamics in Nature and Society, 2017: 1-14.

[12] KUMARI S, UPADHYAY R K. Exploring the behavior of malware propagation on mobile wireless sensor networks: stability and control analysis[J]. Mathematics and Computers in Simulation, 2021, 190: 246-269.

[13] ZHU Q Y, ZHANG G, LUO X H, et al. An industrial virus propagation model based on SCADA system[J]. Information Sciences, 2023, 630: 546-566.

[14] KABIR S, PAPADOPOULOS Y. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: a review[J]. Safety Science, 2019, 115: 154-175.

[15] PASANDIDEH S, GOMES L, MALO P. Improving attack trees analysis using Petri net modeling of cyber-attacks[C]//Proceedings of the 2019 IEEE 28th International Symposium on Industrial Electronics (ISIE). Piscataway: IEEE Press, 2019: 1644-1649.

[16] 姜文淇. 基于改进Petri网的工业机器人系统风险评估方法研究[D]. 哈尔滨: 哈尔滨工业大学, 2021.
JIANG W Q. Research on risk assessment method of industrial robot system based on improved Petri net[D]. Harbin: Harbin Institute of Technology, 2021.

[17] FLAMMINI F, GENTILE U, MARRONE S, et al. A Petri net pattern-oriented approach for the design of physical protection systems[C]//Computer Safety, Reliability, and Security. Cham: Springer International Publishing, 2014: 230-245.

[18] DUIJM N J. Safety-barrier diagrams as a safety management tool[J]. Reliability Engineering & System Safety, 2009, 94(2): 332-341.

[19] BADREDDINE A, BEN ROMDHANE T, BEN HAJKACEM M A, et al. A new multi-objectives approach to implement preventive and protective barriers in bow tie diagram[J]. Journal of Loss Prevention in the Process Industries, 2014, 32: 238-253.

[20] FERDOUS R, KHAN F, SADIQ R, et al. Handling and updating uncertain information in bow-tie analysis[J]. Journal of Loss Prevention in the Process Industries, 2012, 25(1): 8-19.

[21] IEC/SC 65A. IEC EN 61508-2010: Functional safety of electrical/electronic/programmable electronic safety-related systems[S]. IEC: IEC, 2010.

[22] 马叶桐, 丁云杰, 刘圃卓, 等. 工业控制系统功能安全和信息安全一体化风险评估方法[J]. 信息安全学报,2021.
MA Y T, DING Y J, LIU P Z, et al. Integrated risk assessment algorithm for functional safety and information security of industrial control systems[J]. Journal of Cyber Security. 2021.

[23] LYU X R, DING Y L, YANG S H. Safety and security risk assessment in cyber-physical systems[J]. IET Cyber-Physical Systems: Theory & Applications, 2019, 4(3): 221-232.

[24] ONISAWA T. An approach to human reliability in man-machine systems using error possibility[J]. Fuzzy Sets and Systems, 1988, 27(2): 87-103.

[25] BADIDA P, BALASUBRAMANIAM Y, JAYAPRAKASH J. Risk evaluation of oil and natural gas pipelines due to natural hazards using fuzzy fault tree analysis[J]. Journal of Natural Gas Science and Engineering, 2019, 66: 284-292.

[26] Forum of Incident Response and Security Teams. Common vulnerability scoring system version 3.1: specification document[R]. 2021.

[27] MUÑOZ-GONZÁLEZ L, SGANDURRA D, BARRÈRE M, et al. Exact inference techniques for the analysis of Bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(2): 231-244.

[28] FORMBY D, RAD M , BEYAH R. Lowring the barriers to industrial control system security with GRFICS[C]//Proceedings of USENIX Workshop on Advances in Security Education (ASE).2018.

[29] RICKER N L. Model predictive control of a continuous, nonlinear, two-phase reactor[J]. Journal of Process Control, 1993(3):109-123.

[30] ALVARO A, CÁRDENAS, AMIN S, et al. Attacks against process control systems: risk assessment, detection, and response[C]//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security(ASIACCS' 11). New York: ACM Press, 2011:355-366. doi:10.1145/1966913.1966959.

[作者简介]

王红敏（1989– ），女，信息工程大学讲师，主要研究方向为工业控制系统安全入侵检测、风险评估。

韩少云（1991– ），男，博士，河南工程学院讲师，主要研究方向为工业软件安全、机器学习、数据挖掘。

魏强（1979– ），男，博士，信息工程大学教授，主要研究方向为网络与信息系统安全、软件脆弱性分析、云计算安全、工控系统安全、智能终端安全、软件定义网络等。

宋思静（2000– ），女，信息工程大学博士生，主要研究方向为工业控制系统协议安全。