计算机科学
COMPUTER SCIENCE

SSPN-RA:基于SS-petri网的工业控制系统安全一体化风险评估方法

马梓刚, 麻荣宽, 李贝贝, 谢耀滨, 魏强, 彭慜威

引用本文

马梓刚, 麻荣宽, 李贝贝, 谢耀滨, 魏强, 彭慜威. SSPN-RA:基于SS-petri网的工业控制系统安全一体化风险评估方法[J]. 计算机科学, 2024, 51(10): 380-390.

MA Zigang, MA Rongkuan, LI Beibei, XIE Yaobin, WEI Qiang, PENG Minwei. SSPN-RA:Security Integration Risk Assessment Method for ICS Based on SS-petri Net [J]. Computer Science, 2024, 51(10): 380-390.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231000189

SSPN-RA:基于SS-petri网的工业控制系统安全一体化风险评估方法

马梓刚[1]　麻荣宽[1]　李贝贝[2]　谢耀滨[1]　魏　强[1]　彭憨威[1]
1 信息工程大学网络空间安全学院　郑州 450001
2 四川大学网络空间安全学院　成都 610065
(gang15950362616@qq.com)

摘　要　随着信息化与工业化的融合不断加深,工业控制系统中信息域与物理域交叉部分越来越多,传统信息系统的网络攻击会威胁工业控制系统网络。传统的工业控制系统安全评估方法只考虑功能安全的风险,而忽略了信息安全风险对功能安全的影响。文中提出一种基于改进petri网的工业控制系统功能安全和信息安全一体化风险建模方法(Safety and Security Petri Net Risk Assessment,SSPN-RA),其中包括一体化风险识别、一体化风险分析、一体化风险评估3个步骤。所提方法首先识别并抽象化工业控制系统中的功能安全与信息安全数据,然后在风险分析过程中通过构造结合Kill Chain的petri网模型,分析出功能安全与信息安全中所存在的协同攻击路径,对petri网中功能安全与信息安全节点进行量化。同时,通过安全事件可能性以及其造成的各类损失计算出风险值,实现对工业控制系统的一体化风险评估。在开源的仿真化工工业控制系统下验证该方法的可行性,并与功能安全故障树分析和信息安全攻击树分析进行对比。实验结果表明,所提方法能够定量地得到工业控制系统的风险值,同时也解决了功能安全与信息安全单一领域分析无法识别的信息物理协同攻击和安全风险问题。

关键词:风险评估;petri网;工业控制系统;安全一体化;功能安全;信息安全
中图分类号　TP309

SSPN-RA:Security Integration Risk Assessment Method for ICS Based on SS-petri Net

MA Zigang[1],MA Rongkuan[1],LI Beibei[2],XIE Yaobin[1],WEI Qiang[1] and PENG Minwei[1]
1 School of Cyber Security,Information Engineering University,Zhengzhou 450001,China
2 School of Cyber Science and Engineering,Sichuan University,Chengdu 610065,China

Abstract　With the continuous integration of informatization and industrialization,there are more and more intersecting parts between information domain and physical domain in industrial control systems,and network attacks on traditional information systems will threaten the industrial control system network. Traditional industrial control systems only consider the risks of functional safety,ignoring the impact of information security risks on functional safety. This paper proposes an integrated risk modeling method for functional safety and information security of industrial control system named SSPN-RA based on improved petri net,which includes three steps:integrated risk identification,integrated risk analysis and integrated risk assessment. This paper firstly identifies and abstracts the functional safety data and information safety data in the industrial control system,and then analyzes the collaborative attack path of functional safety and information security by constructing the petri net model combined with Kill Chain in the risk analysis process. Subsequently it quantifies the functional safety and information security nodes in the petri net,and finally calculates the risk value through the possibility of safety events and various losses caused by these safety events,so as to complete the integrated risk assessment of the industrial control system. In this paper,the feasibility of the proposed method is verified under the open-source simulation of chemical tank industrial control system,and compared with fault tree analysis and attack tree analysis. Experimental results show that the proposed method can quantitatively obtain the risk value of industrial control system,and also solve the problem of cyber-physical collaborative attack and security risk that cannot be identified by the analysis of functional safety and information security.

Keywords　Risk assessment,Petri net,Industrial control system,Security integrity,Functional safety,Information security

到稿日期:2023-10-27　返修日期:2024-03-23
基金项目:国家重点研发计划(2020YFB2010900);中原科技创新领军人才项目(224200510002)
This work was supported by the National Key R&D Program of China(2020YFB2010900) and Program for Innovation Leading Scientists and Technicans of Zhongyuan(224200510002).
通信作者:麻荣宽(rongkuan307@163.com)

1 引言

工业控制系统(Industrial Control System，ICS)是一类由多种控制系统及相关仪器设备共同构成的，用于确保工业基础设施自动化运行、过程监控的业务流程管控系统。ICS 已被广泛部署并应用于燃气、电力、水利、化工、制药、食品等关键基础设施领域，成为推动世界发展的重要力量。

工业化与信息化的融合与发展[1]，加快了传统制造业中引入信息技术的进程，打破了原本的“孤岛隔离”式网络业务形态[2]。信息系统中存在的网络攻击也进而向工业控制系统网络渗透，这对没有采取安全设计和安全防护措施的工业控制系统产生了比较严峻的安全危害。“Stuxnet”[3]是第一个定向攻击真实世界基础设施的恶意代码，为工业控制系统的安全生产敲响了警钟。“Stuxnet”利用多个零日漏洞，突破了系统的“物理隔离”，打破了信息域和物理域的边界，篡改了工业控制器中的控制逻辑程序，最终对物理设备造成破坏。“Duqu”“Flame”“Havex”等工控安全事件也随之发生。这些事件表明，工业控制系统面临物理和信息两个角度的双重破坏风险。

对工业控制系统进行风险评估，是为了识别已存在的安全风险以及针对未知的安全风险作出决策。工业控制系统的风险评估分为功能安全风险评估和信息安全风险评估，两者在风险评估对象、风险来源、风险后果、风险分析、参考标准和安全分级等方面存在不同之处，具体如表 1[4-5]所列。

表 1 功能安全风险评估与信息安全风险评估比较

Table 1 Risk assessment comparison of functional safety and information security

	功能安全风险评估	信息安全风险评估
评估对象	安全相关控制系统/受控设备	生产过程区域和管道
评估来源	功能失效、组件故障失效时间	威胁：系统内部或外部 脆弱性：组件或系统存在的安全漏洞
风险分析	定量分析	定性分析
参考标准	IEC61508 等	IEC62443 等
安全分级	安全完整性等级(SIL)	安全等级(SL)

工业控制系统功能安全风险评估主要分析系统内部的故障风险，主要分析方法[4-6]有：ALARP 方法(As Low As Reasonably Practicable，ALARP)、保护层分析方法(Layer Of Protection Analysis，LOPA)、危害与可操作性分析(Hazard And Operability Study，HAZOP)、失效模式与影响分析(Failure Mode and Effects Analysis，FMEA)等。功能安全风险的缓解方法是参考 IEC 61508[7]等标准进行风险定量分析后，依据安全完整性等级(SafetyIntegrity Level，SIL)目标制定措施。信息安全风险评估主要分析系统所面临的外部威胁，主要分析方法[6]有：因果分析(Cause-consequence Analysis)模型、攻击树(Attack Tree，AT)模型等。信息安全风险的缓解方法是针对生产过程的区域和管道，识别区域和管道的机密性、完整性和可用性面临的安全威胁属性和脆弱性的严重程度，对资产存在的漏洞利用的可能性及漏洞利用成功的后果进行定性分析，并根据安全等级(Security Level，SL) 制定措施。

无论是功能安全风险评估还是信息安全风险评估，都是从一个角度考虑的单一的风险评估。功能安全风险评估中缺乏对信息域威胁触及至物理域风险的评估，而信息安全风险评估也未能准确衡量对功能安全的影响；并且，随着工业化与信息化的融合，单方面的功能安全风险评估或信息安全风险评估，很难对信息物理协同的攻击风险进行识别。

由于没有功能安全与信息安全一体化风险评估相关标准的指导，因此相关的研究也仅从定性的角度分析工业控制系统中的风险，未有一个有效或合理的计算方式来从功能安全与信息安全一体化的角度计算其相应的风险值。本文提出一种工业控制系统安全一体化风险评估方法，定量地分析工业控制系统中的功能安全与信息安全相关的数据，同时基于 petri 网并结合 Kill Chain 模型生成协同攻击路径，用于风险值的计算。本文提出的安全一体化风险评估方法与传统风险评估类似，包含风险识别、风险分析、风险评估 3 个步骤。首先，通过自动化工具或人为查询的方式，收集来自于工业控制系统中的有关功能安全与信息安全的风险数据。接着，在风险分析阶段，利用 petri 网并结合 Kill Chain 模型形成 SS-petri 网，生成工业控制系统中可能存在的信息物理协同攻击路径，提出可行的计算方式计算出工业控制系统的风险值。最后，在风险评估阶段，综合评估其风险等级。

本文的主要贡献包括：

(1)提出一种基于 petri 网并结合 Kill Chain 模型的工业控制系统功能安全与信息安全一体化风险评估方法 SSPN-RA，实现对物理域故障失效风险与信息域网络攻击一体化的定量分析。

(2)将 petri 网结合 Kill Chain 模型应用在功能安全与信息安全一体化风险分析中，能够对工业控制系统中的资产、威胁、故障事件进行分析，并引入贝叶斯概率计算工业控制系统风险值。

(3)在一个仿真的化工罐系统中实现对一体化风险评估方法的验证，结果表明，一体化风险分析方法能够有效识别信息域和物理域存在耦合的风险，并分析出最有可能的信息物理协同攻击产生的安全事件。通过与功能安全的故障树分析、信息安全的攻击树分析比较可以发现，一体化安全分析方法能更加全面地分析风险。

2 相关工作

有关工业控制系统风险评估的研究主要包含 3 类：功能安全风险评估[8-11]、信息安全风险评估[12-15]和融合功能安全与信息安全的风险评估[16-21]。

部分标准中提到了有关工业控制系统的安全完整性等级验证的方法。安全完整性等级的划分实质上就是一种针对风险的评估，如 ALARP 方法、LOPA 方法等，通过失效时间对其进行计算，得出相应的等级。传统的功能安全评估方法还包括失效模式与影响分析、故障树分析(Fault Tree，FT)等。随着工控系统的复杂化，贝叶斯网络以及 petri 网等风险建模方法也被应用在此类风险评估中。文献[8]提出基于模型的时间故障树来增强故障树的表达能力，捕捉完整的系统故障行为，并通过飞机燃料分配系统来证明其有效性。文献[9]将

模糊理论应用于故障树分析，解决了历史数据不足的问题；文献[10]利用贝叶斯网络和博弈论相结合的风险评估方法，全面评估系统的自身功能安全问题与来自第三方的功能安全干扰；文献[11]提出一种四步的基于安全完整性水平(SIL)的分析方法，对水下控制系统的功能模块进行风险评估。

在信息安全风险评估中，使用的方法与功能安全风险评估类似，例如改进故障树为攻击树等，但大多是针对工业控制系统下的网络安全进行风险评估。文献[12]提出了一个基于贝叶斯网络的信息安全风险评估模型，其可以从历史数据中通过增量学习提高风险评估的准确性并评估未知的网络攻击。文献[13]在贝叶斯网络中结合模糊概率，动态地评估工业控制系统的信息安全，并在化学反应器控制系统中进行了实验。文献[14]在贝叶斯网络中设计了一种新的基于多模型的危险事件预测方法，对工业控制系统进行信息安全风险评估。文献[15]从资产的功能属性出发，结合 petri 网分析网络攻击的影响传播，在对化工控制系统的仿真研究中证明了此方法的有效性。

在一体化风险评估的研究中，文献[16]提出了 FMEAV 方法，改进传统的失效模式与影响分析(FMEA)为失效/威胁分析和失效链，并提出了对信息安全的威胁链及具体评判标准。文献[17]在功能安全的分析方法危险与可操作性(hazop)之中添加了部分元素，使得其能够应用于信息安全的场景中。但这些方法只是简单地改进了功能安全风险评估方法的部分，而未考虑功能安全与信息安全交互与冲突的地方。

对此，部分学者提出了融合功能安全与信息安全的解决方案。文献[18]提出了集成六步模型与信息流图的方法。六步模型用关系矩阵识别不同层次之间的关系，并确定故障及网络攻击对系统的影响，加入信息流图对其进行改进，使其能够同时识别故障和攻击，并通过 SWAT 系统验证了方法的可行性。文献[19]将蝴蝶结分析法和扩展的攻击树分析法进行组合，蝴蝶结分析用于功能安全方面的分析，攻击树用于信息安全方面的分析；并在化工场景下验证了此方法。文献[20]先将整个控制回路定为控制层，在分析功能安全后，根据相应的联系对网络安全进行分析，最终得到系统整体策略，并在电网场景中验证了这一方法。文献[21]提出了 S-cube 框架，通过知识库对网络物理系统的物理和功能架构进行正式建模，自动生成包含功能安全风险和信息安全风险的定性和定量分析；并在典型的工控架构下验证了方法的有效性。文献[22]提出了用扩展攻击树的方式定量分析工业控制系统中的一体化安全，并在燃气管网环境中验证了其合理性。

然而，上述的有关研究中都未提出合理的计算安全一体化的结果，也没有构造具体的模型或提出相应的计算方式，仅从定性的角度分析工业控制系统的功能安全与信息安全，仍然存在缺陷，风险分析得出的结果不够直观，也难以通过具体的内容提出可行的解决措施。

本文针对相关领域研究的不足，提出了功能安全与信息安全一体化定量分析方法，通过识别并抽象化功能安全与信息安全风险数据，在 petri 网中结合 Kill Chain 模型[22]对工业控制系统识别的数据进行一体化安全分析，得到信息物理协同攻击产生的安全事件，同时考虑功能安全与信息安全的风险损失，定量地得到工业控制系统风险值。本文所提方法不仅解决了一体化安全风险评估中不能一体化定量分析的问题，同时也为如何识别物理域和信息域互相影响的风险事件提供了思路。

3 基于 SS-petri 网的工控系统安全一体化风险评估方法

本章介绍了基于 petri 网的工业控制系统安全一体化风险评估方法，包括一体化风险识别、一体化风险分析、一体化风险评估 3 个步骤。一体化风险评估方法的原理如图 1 所示。

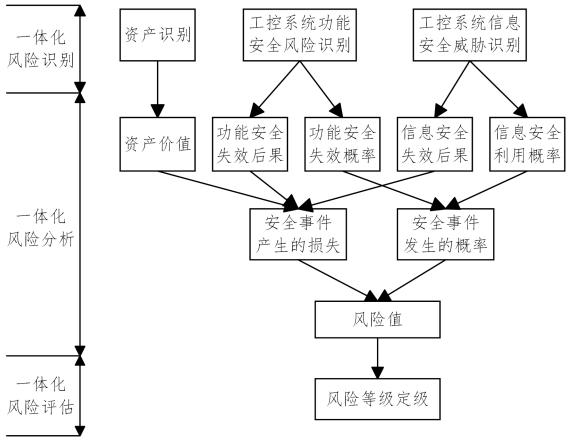


图 1 一体化风险评估方法原理

Fig. 1 Principles of integrated risk assessment method

一体化风险识别的过程包括资产识别、功能安全风险识别和信息安全威胁识别。一体化风险分析，通过安全事件产生的损失和安全事件发生的概率两个指标得到工业控制系统的风险值，而产生的损失由识别到的资产价值、功能安全失效后果和信息安全失效后果 3 类指标得到，安全事件发生的概率由功能安全失效概率和信息安全利用概率 2 类指标确认。最后的一体化风险评估通过分析所得到的风险值进行判定，从而给出工业控制系统应当采取的措施。

3.1 安全一体化风险识别

本节介绍安全一体化风险评估的第一步：安全一体化风险识别。首先介绍功能安全来源和信息安全来源的风险信息的数据集来源，接着对风险数据进行抽象化描述。

风险数据识别是进行风险评估的基础。在之前的相关研究工作中，此步骤一般只收集信息安全相关的威胁数据信息。本文提出的安全一体化风险评估方法则从多个不同数据集中同时收集功能安全来源的风险数据和信息安全来源的风险数据，并对一体化风险数据进行抽象化描述，从而实现了安全一体化风险识别的过程。

3.1.1 风险识别的数据来源

功能安全与信息安全的风险数据集来源分别描述如下。

功能安全数据集信息主要包含：

(1)工业控制系统中有关 SIL 等级验证的数据；

(2)工业控制系统中保证系统运行的功能安全的组件

各类要求，如温度、压强、湿度、防尘等；

(3)人员操作失误等人为原因；

(4)阀门、警报器故障等机械故障；

(5)工控设备及组件的官方手册等。

信息安全数据集信息主要包含：

(1)工业控制系统中设备存在的信息安全漏洞：CVE，CWE 和 CNVD 中查询设备对应的漏洞编号及利用难度；

(2)通讯协议漏洞：设备所使用的通讯协议存在安全漏洞；

(3)在 ATT&CK for ICS 等安全知识库中收集到的针对设备的探测、瘫痪、泄露等攻击技术；

(4)人为方面的失误；

(5)工控系统网络拓扑结构。

3.1.2 数据的抽象化描述

(1)资产：资产中包含 *id*，用于身份标识；*safety_risk* 与 *security_risk* 分别表示资产中存在的功能安全风险集与信息安全风险集。资产具体描述为：

$$Asset=(id,safety\_risk,security\_risk) \tag{1}$$

(2)风险：资产中存在的功能安全风险 *Safety_Risk* 与信息安全风险 *Security_Risk*，其中 *safety* 表示系统存在的功能安全故障，*safety_path* 表示功能安全失效的路径。功能安全风险和信息安全风险分别描述为：

$$Safety\_Risk=(safety,safety\_path) \tag{2}$$

$$Security\_Risk=(security,security\_path) \tag{3}$$

(3)攻击者：工业控制系统中可能会受到攻击的起点，是将要构造的攻击路径的起始点，所有不同的攻击路径综合构成基于 Kill Chain 的攻击路径 petri 网。*local* 表示攻击者来源，例如外部黑客或内部恶意工作人员；*privilege* 表示攻击者所具有的权限。攻击者描述为：

$$Attacker=(local,privilege) \tag{4}$$

(4)信息安全脆弱集：*security_id* 表示信息安全中存在的漏洞标识，例如 *CVE* 编号，*id* 表示与资产相关的标识；*att_stage* 表示信息安全风险点位于 Kill Chain 中侦察追踪、武器构建、载荷投递、漏洞利用、安装植入、持续控制和目标达成 7 个攻击阶段之一[22]。信息安全脆弱集描述为：

$$Security=(security\_id,id,att\_stage) \tag{5}$$

(5)功能安全故障集：*safety_id* 表示功能安全中存在的失效风险，*id* 表示与资产相关的标识，*failure_stage* 表示功能安全风险点中的失效状态(改进于 Kill Chain，描述为几个失效阶段：初始失效、失效传递、达到最终失效目标)。功能安全故障集描述为：

$$Safety=(safety\_id,id,failure\_stage) \tag{6}$$

(6)功能安全与信息安全路径集：通过分析基于 petri 网的 Kill Chain 模型得到工业控制系统功能安全与信息安全风险事件，其中 p 代表 petri 网中的库所，t 代表 petri 网中的变迁。功能安全与信息安全路径集描述为：

$$Safety\_path=(path_1,\cdots,path_n) \tag{7}$$

$$Security\_path=(path_1,\cdots,path_n) \tag{8}$$

3.2 安全一体化风险分析

安全一体化识别之后，就是对工控系统进行风险分析。风险分析从风险源头、风险点及最后的风险结果等方面详细考虑，进而确定工业控制系统的风险水平。风险分析分为定量分析和定性分析，常用的分析方法包括故障树[23]分析(Fault Tree，FT)、攻击树(AttackTree，AT)模型[24]、贝叶斯网络[25]、蝴蝶结(Bow-Tie，BT)[26]分析法、事件树分析 ETA 等。

本文所用到的安全一体化风险分析子模型是基于 petri 网的 Kill Chain 模型，主要包括 petri 网的 Kill Chain 模型的生成以及依据生成的模型对工业控制系统进行风险值的计算两个步骤。其中，风险识别的输出数据会作为风险分析模型的输入，风险分析模型的输出则是基于 petri 网的 Kill Chain 模型计算得到的风险水平。

安全一体化风险分析子模型通过在 Kill Chain 模型中构建一个融合功能安全与信息安全的攻击路径，分析安全事件发生的概率；接着计算功能安全与信息安全两者的损失，其中功能安全包涵对人员、资产、环境的影响，信息安全包涵对信息资源的机密性、完整性、可用性的影响，从而实现了安全一体化风险分析。

3.2.1 基于 SS-petri 网的工业控制系统攻击路径生成

petri 网模型在描述异步、离散、并发的计算机系统时具有优势。攻击者会根据已有的资源对工业控制系统进行阶段性渗透破坏；且工业控制系统中各个设备的安全状态随时间变化，无法用连续函数进行描述；工业控制系统的各个资产的安全状态具有潜在的关联性，资产安全状态的变化只依赖于外延，与全局情况无关。因此，针对工业控制系统的攻击行为也具有异步、离散、并发的性质。通过结合工业控制系统 Kill Chain 模型构造工业控制系统的 petri 网是可行的方案。

一个简单的攻击行为及其 petri 网描述模型如图 2 所示。攻击者利用工业控制器存在的漏洞对工业系统中的 PLC 进行攻击，将该过程抽象为 petri 网模型，则 petri 网内的变迁元素 t 代表利用漏洞攻击 PLC，petri 网内的库所元素 p 代表所存在的漏洞。

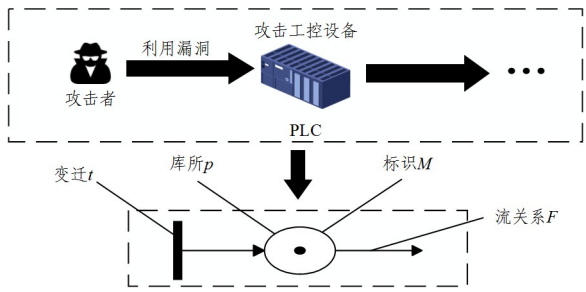


图 2 工控攻击行为及其 petri 网描述

Fig. 2 Industrial control attack behavior and its PN description

通过图 2，可以给出如下定义：

(1)petri 网内的变迁集 $T=\{t_1,t_2,\cdots,t_n\}$，对应到工业控制系统中的有关功能安全与信息安全的全部威胁 $Th=\{Th_1,Th_2,\cdots,Th_n\}$；

(2)petri 网内库所集 $P=\{P_1,P_2,\cdots,P_n\}$ 对应于工业控制系统中有关功能安全的全部失效性 $Fa=\{Fa_1,Fa_2,\cdots,$

$Fa_n\}$与信息安全的全部脆弱性 $Vu=\{Vu_1,Vu_2,\cdots,Vu_n\}$；

(3)对于 petri 网内任意一个库所 $p\in P$，其当前标记 $M(p)$对应于工业控制系统对脆弱性 Vu 在 Kill Chain 的状态 Att_Stage，例如：载荷投递、漏洞利用、目标达成。

通过识别的风险数据进行基于 petri 网的 Kill Chain 建模，建模方法原理如图 3 所示。实施步骤包括：

(1)根据风险识别的数据构建工业控制系统网络模型、工控系统资产集 $Asset$、威胁集 Th、脆弱性集 Vu、故障集 Fa、路径集 Pa、攻击者 At。

(2)构建攻击者队列 Q_{at}、脆弱集队列 Q_{Vu}、故障集队列 Q_{Fa}、威胁集队列 Q_{Th}，并取出攻击者 At 中的元素作为 petri 网的初始节点对象 p。

(3)判断下一个创建的节点是否为信息安全脆弱集。若是，从脆弱性队列 Q_{Vu} 抽象 Vu_i 为库所 p_i，否则从故障集队列 Q_{Fa} 抽象功能安全故障 Fa_j 为 p_j。

(4)判断对应资产的 Q_{Vu} 和 Q_{Fa} 队列是否为空，若是则转向步骤(5)，否则重复步骤(3)，继续生成 petri 网模型。

(5)判断攻击队列是否为空。若是，则添加相邻库所对应于威胁队列 Q_{Th} 的变迁 t_i，将 petri 网模型完成；否则转向步骤(2)，继续构造 petri 网模型。

(6)通过构造完基于 petri 网的 Kill Chain 模型，从初始节点攻击者，到达最终信息安全状态的目标达成，和到达最终功能安全状态的目标失效状态，生成不同路径的 Pa 集合。

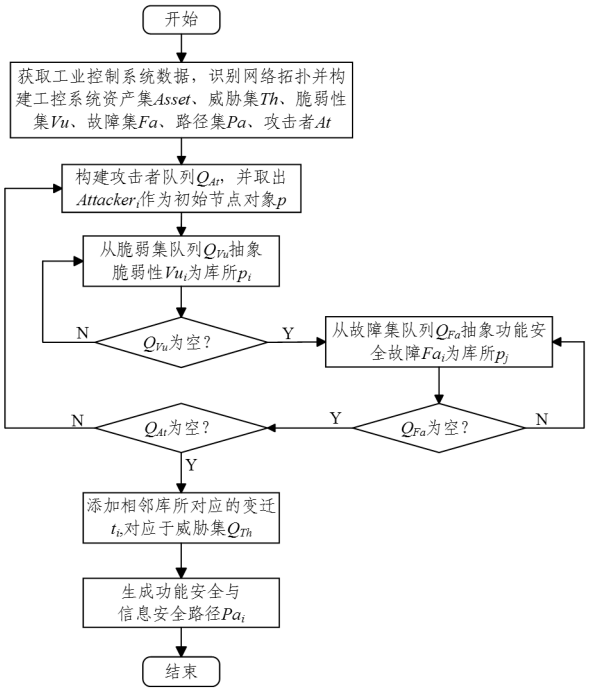


图 3 SS-Petri 网建模方法原理图

Fig. 3 Schematic diagram of SS-Petri net modeling method

3.1.2 风险分析与计算

根据上述方式成功构造 petri 网后，接着对得到的 petri 网进行系统级的风险分析与计算，主要包括 3 个子步骤。

(1)对 petri 网中初始节点攻击难度和故障失效的量化

对模型中初始节点的攻击难度的量化，在本文中定义为攻击者利用功能安全失效或信息安全漏洞对 SS-petri 网模型的初始节点进行一次功能安全失效风险的产生或进行一次信息安全漏洞的利用的难易程度的量化，因此初始节点故障失效或攻击难度应从功能安全风险失效率与信息安全漏洞利用难度两方面进行考虑。

首先是对信息安全漏洞利用难度的量化。通用漏洞评分系统(Common Vulnerability Scoring System，CVSS) 是一个公开的标准框架，用于测评漏洞的特征和严重程度，在部分漏洞网站中可以查询到相关漏洞的 CVSS 得分，包括 Base，Temporal 和 Environmental3 个属性。Base 表示漏洞本身的基础属性，Temporal 反映随时间变化的漏洞特征，Environment 表示用户环境所特有的漏洞特征，3 个属性会用到不同的要素以及分数计算公式。Base 度量标准组得出一个值在 0～10 范围内的分数，后续可以通过 Temporal 和 Environmental 度量标准组评分进行修改[27]。

Base 属性包含可利用性指标(Exploitability Metrics)、影响指标(Impact Metrics)和范围(Scope)3 个部分，如图 4 所示。其中可利用性指标包含的要素常用于漏洞攻击难度的量化，包括攻击向量(Attack Vector，AV)、攻击复杂性(Attack Complexity，AC)、需要权限(PrivilegesRequired，PR)和用户交互(User Interaction，UI)等。本文选择上述 4 个与漏洞利用相关的要素对信息安全漏洞利用攻击难度进行量化计算。

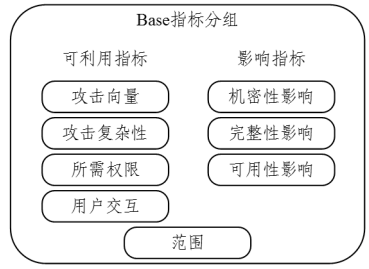


图 4 Base 指标分组

Fig. 4 Base index grouping

如表 2 所列，CVSS 将这 4 类要素划分为不同等级，并进行相应的数值量化[27]。

表 2 信息安全中指标的描述及数值量化

Table 2 Description of indicators in information security and numerical quantization

要素	要素等级描述	数值量化
攻击向量(AV)	物理访问	0.20
	本地访问	0.55
	相邻网络访问	0.62
	远程网络访问	0.85
攻击复杂性(AC)	高	0.44
	低	0.77
所需权限(PR)	高	0.27
	低	0.62
	无	0.85
用户交互(UI)	需要	0.62
	无	0.85

参考 CVSS 的分数计算过程[27]，计算信息安全风险利用难度的值，并进行归一化处理：

$$Basescore(p)=\frac{8.22\times AV\times AC\times PR\times UI}{10} \tag{9}$$

然后根据信息安全漏洞的利用难度的指标及 CVSS 的量化方式，提出有关功能安全故障失效的 4 类指标，并对 4 个指标进行描述及数值量化，如表 3 所列。

表 3 功能安全中指标的描述及数值量化

Table 3 Description of indicators and numerical quantization in functional safety

要素	要素等级描述	数值量化
组件 SIL 等级 (S)	无	0.1
	SIL1	0.01
	SIL2	0.001
	SIL3	0.0001
	SIL4	0.00001
意外事件影响 (A)	无	1
	高	0.1
	中	0.01
	低	0.001
环境影响 (E)	无	1
	高	0.1
	中	0.01
	低	0.001
人为失误影响 (P)	无	1
	高	0.6
	中	0.2
	低	0.01

本文将功能安全失效分为 4 类：组件本身出现了问题参考其安全完整性等级 SIL，由特殊情况产生的事故导致功能安全失效的意外事件影响 A，由环境因素例如温度压强等导致的失效为 E，人为失误产生的影响 P。对功能安全失效概率的计算由 4 个要素组成。

因此参考表 3 与信息安全风险利用难度计算式，提出功能安全失效概率的计算式如下：

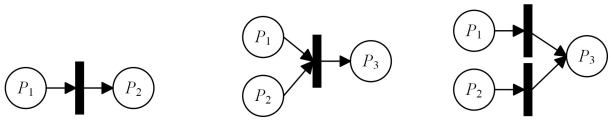
$$Basescore(p)=S\times A\times E\times P \tag{10}$$

综合上述两种计算方式得到初始节点的计算式如下：

$$Basescore(p)=\begin{cases}\dfrac{8.22\times AV\times AC\times PR\times UI}{10}, & p\in Vu\\ S\times A\times E\times P, & p\in Fa\end{cases} \tag{11}$$

(2)条件节点和原子攻击节点的局部条件概率分布计算

在工业控制系统 Kill Chain 模型中，由于连接关系的库所具有因果关系，因此引入贝叶斯概率，对攻击发生的概率进行推理。两类推理模型如图 5 所示。



(a)顺序逻辑 (b)与逻辑 (c)或逻辑

图 5 petri 网推理模型

Fig. 5 Inference model of petri net

以图 5(b)为例，说明本文中的推理原理。由于 P_1 和 P_2 可以推导出 P_3，因此 P_1 和 P_2 是 P_3 的父代库所，记作：

$$Par(P3)=\{P1,P2\} \tag{12}$$

不同父代库所逻辑的贝叶斯推理计算公式不同。对于工业控制系统内库所 P_i，其父代库所集合为 $Par(P_i)$。若 $Par(P_i)$ 的关系为“AND”，则：

$$P(P_i\mid Par(P_i))=\begin{cases}0, & \exists P_i\in Par(P_i),P_i=0\\ \prod\limits_{i=1}^{i}Par(P_i), & \text{otherwise}\end{cases} \tag{13}$$

如图 5(c)所示，$Par(P_i)$ 的关系为“OR”，则：

$$P(P_i\mid Par(P_i))=\begin{cases}0, & \forall P_i\in Par(P_i),P_i=0\\ 1-\prod\limits_{i=1}^{i}[1-Par(P_i)], & \\ & \text{otherwise}\end{cases} \tag{14}$$

(3)功能安全风险传播路径或信息安全攻击路径的风险值计算

首先对事件发生的可能性进行计算。已知工业控制系统 SS-petri 网模型中某条路径发生的可能性，是这条路径上所有节点的联合概率分布。根据贝叶斯定理[28]，假设某条路径包含 1,2,…,k 节点，则此条路径发生的可能性 P 的计算式如下：

$$P=P(x_1,x_2,\cdots,x_k)=P(x_k\mid x_1,x_2,\cdots,x_{k-1}),\cdots,P(x_2\mid x_1)P(x_1) \tag{15}$$

假设目标达成状态的节点是由 k 条路径并结合某种功能安全风险失效传播或信息安全漏洞利用方式引起的，则事件发生的概率 SP 的计算式如下：

$$SP=\sum_{i=1}^{k}P_i\times\beta_i \tag{16}$$

其中，P_i 表示第 i 条路径发生的可能性；β_i 表示取得第 i 条路径权限下，选取某种功能安全失效风险传播或信息安全漏洞利用方式的可能性。

计算事件发生的可能性后，对事件的影响后果进行计算。事件的影响一般通过事件造成的损失来体现，分为功能安全损失和信息安全损失两种，包括对人员、资产、环境的影响和对信息资源的机密性、完整性、可用性的影响等等。损失 L 量化引入 λ_1，λ_2，λ_3 3 个变量，用于区分事件带来的资产损失、人员损失和信息安全损失。损失 L 的计算式如下：

$$L=\lambda_1\ I_a+\lambda_2 I_p+\lambda_3 I_s \tag{17}$$

其中，λ_1，λ_2，λ_3 表示资产损失、人员损失和信息安全损失分别对应的加权系数；I_p 表示人员损失的归一化结果；I_s 表示信息安全机密性、完整性、可用性损失；I_a 表示资产损失，由式(18)求得：

$$I_a=a_1\times\frac{N_1}{N}+a_2\times\frac{N_2}{N},\ a_1+a_2=1 \tag{18}$$

其中，I_a 表示资产的重要度，N_1 和 N_2 分别表示事件发生后仍可运行的资产和无法运行的资产的数目，N 表示资产总数目，a_1 和 a_2 为相对应的加权系数且 $a_1+a_2=1$。

因此，事件风险值的计算式如下：

$$risk_n=SP_n\times L_n \tag{19}$$

其中，SP_n 表示第 n 个事件发生的概率，L_n 表示第 n 个事件发生时对系统的影响。

工业控制系统最易发生的事件以风险值为依据，风险值最大的即为系统最易发生的事件。系统的风险值取值为系统

最易发生事件的风险值，其计算式如下：

$$Risk=max\{risk_1,risk_2,\cdots,risk_n\} \tag{20}$$

其中，$risk_i$ 表示第 i 个事件的风险值；n 为系统事件的总数；$Risk$ 为系统最易发生的事件的风险值，即系统的风险值。

综上所述，最后风险分析模型的输出即为基于 SS-petri 网模型与根据模型计算得出的工业控制系统风险值 $Risk$ 。

3.3 安全一体化风险评估

本节介绍安全一体化风险评估方法的安全一体化风险评估，首先进行风险等级划分，然后根据风险等级采取不同措施。通过安全一体化风险识别及安全一体化风险分析，根据已有的数据得到工业控制系统风险值 $Risk$，以及系统发生风险的可能性和影响程度，确定系统风险等级，同时决定是否需要采取控制措施等。

国家标准[29]中提出对风险评估的结果进行等级化处理。按照风险值的高低进行等级划分，风险值越大，风险等级越高。一般划分为 5 个等级。

根据文献[30]对工业控制系统风险进行等级划分，并根据所得风险等级，采取不同的行动要求，总体描述如表 4 所列。

表 4 风险值描述及行动要求

Table 4 Risk value description and action requirements

风险值范围	风险等级	行动要求
0～0.2	低	无需采取行动
0.2～0.4	中低	可选择
0.4～0.6	中	可选择
0.6～0.8	中高	采取改进措施
0.8～1	高	立即采取改进措施

部分文献提到针对工业控制系统中功能安全与信息安全风险的缓解措施，从两个角度可分为可用性、可靠性保护技术和机密性、完整性保护技术。在得到风险值后，可采取有关的风险缓解措施对工业控制系统进行安全保护。

4 实验验证

本章主要是依据第 3 章提出的工业控制系统功能安全和信息安全一体化风险评估方法，在搭建的仿真化工罐控制系统[31]中对其进行完整的风险评估，从而验证安全一体化风险评估方法的可行性。首先对实验环境仿真化工罐控制系统进行介绍，之后对实验完整过程进行描述，最后通过与故障树分析方法和攻击树分析方法的对比来分析实验结果。

4.1 实验环境

ICSGRF[32]是一个开源的工业控制系统仿真环境，在本文实验环境中包含 5 个设备及仿真的工业过程，包括 ScadaBr（作为 HMI）、PLC、Chemplant、workstation、pfSense。由于本文主要针对能够融合功能安全与信息安全，因此只考虑工业控制系统中的过程控制系统部分。

信息域包含工程师站、OpenPLC[33]、一个防火墙、一个 HMI 设备及仿真化工罐反应过程设备。其中，设备 1 模拟操作员站，设备 2 模拟监控站。

物理域包括由 OpenPLC 控制的 4 个阀门，分别是 2 个进料阀门、1 个出料阀门和 1 个吹扫阀门。

仿真化工罐控制系统的拓扑结构如图 6 所示，资产表单如表 5 所列。

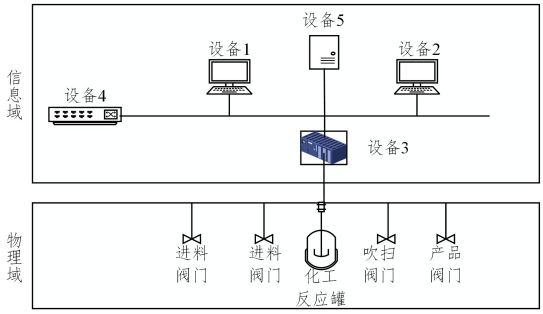


图 6 仿真化工罐控制系统拓扑图

Fig. 6 Topology of simulated chemical tank control system

表 5 化工罐控制系统资产列表

Table 5 Assets in chemical tank control system

资源 id	设备描述
1	workstation
2	scadaBR
3	PLC2
4	pfsense
5	ChemicalPlant

化工罐控制系统通过控制 4 个控制阀门，分别是进料（feed 1）阀门、进料（feed 2）阀门、吹扫阀（purge）阀门和产品（product）阀门，最大限度地提高化学反应的效率，并尽量减少通过吹扫而浪费的组分。

化工罐控制系统的安全事件被定义为由功能安全风险或信息安全风险导致的切断阀未正常关闭，具体情况如下。

安全事件 E_1：在反应罐反应结束后，本应该打开的 purge 和 product 阀门却关闭，使得控制系统出现异常的风险事件。

安全事件 E_2：在反应罐反应进行时，本应该关闭的 purge 和 product 阀门打开，使得反应原料泄露的风险事件。

安全事件 E_3：在反应罐反应进行时，关闭的两个 feed 阀门被打开进行加压，导致化工罐发生爆炸的风险事件。

4.2 实验过程

安全一体化风险评估方法的第一个环节为安全一体化风险数据收集，首先需要确认系统的风险数据来源。本实验选取的功能安全来源的风险数据信息的数据主要包括：

（1）系统网络拓扑结构；

（2）系统元器件参数手册；

（3）系统运行手册；

（4）HRA 分析。

信息安全来源的风险数据信息的数据集主要包括：

（1）利用 nmap 等资产探查扫描工具对系统的资产进行确认；

（2）利用 Nessus[34]项目中的漏洞扫描器 openvas 对系统扫描后得到的漏洞识别结果；

（3）网络攻击链（Cyber Kill Chain）。

依据风险发现、识别与收集的结果，给出系统的风险描述，分别包括系统资产 asset 表（如表 5 所列）、系统信息安全风险表（如表 6 所列）和系统功能安全风险表（如表 7 所列），利用多组表格实现了对系统中设备及设备之间的风险描述。

表 6 信息安全风险

Table 6 Information security risk

Security_id	Vu_{id}	Att_stage	备注
P_5	1	载荷投递	恶意 U 盘掺入
P_6	2	载荷投递	侵入内网
P_7	3	漏洞利用	CVE-2021-41282
P_8	4	漏洞利用	CVE-2020-1938
P_9	5	漏洞利用	CVE-2021-26828
P_{10}	6	漏洞利用	存在漏洞
P_{13}	7	持续控制	获取监控站权限
P_{14}	8	漏洞利用	modbus 栈溢出漏洞
P_{15}	9	持续控制	获取操作者权限
P_{16}	10	持续控制	获取 pfsense 权限
P_{22}	11	持续控制	获取 PLC 权限
P_{27}	12	目标达成	篡改两个进料阀门数据
P_{28}	13	目标达成	篡改两个出料阀门数据
P_{29}	14	目标达成	篡改工程正常程序

表 7 功能安全风险

Table 7 Functional safety risk

Safety_id	Fa_{id}	Att_stage	备注
P_1	1	初始失效	电脑温度异常
P_2	2	初始失效	断电
P_3	3	初始失效	人员误操作
P_4	4	初始失效	机器失效
P_{10}	5	初始失效	PLC 机械失效
P_{11}	6	失效传递	监控站机器失效
P_{12}	7	失效传递	操作员站机器失效
P_{17}	8	失效传递	PLC 失效
P_{18}	9	初始失效	进料 1 阀门机械失效
P_{19}	10	初始失效	进料 2 阀门机械失效
P_{20}	11	初始失效	Purge 阀门机械失效
P_{21}	12	初始失效	Product 阀门机械失效
P_{23}	13	达到最终失效目标	进料 1 阀门失效
P_{24}	14	达到最终失效目标	进料 2 阀门失效
P_{25}	15	达到最终失效目标	Purge 阀门失效
P_{26}	16	达到最终失效目标	Product 阀门失效
P_{30}	17	初始失效	压力传感器失效

风险评估的第二个环节为融合风险分析。首先利用风险识别环节的输出数据集，生成化工罐控制系统 SS-petri 模型，如图 7 所示。系统安全事件对应节点如图 8 所示。

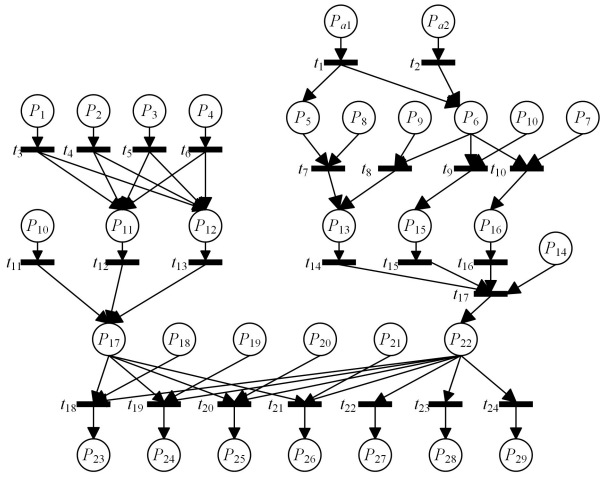


图 7 化工罐控制系统 SS-petri 模型

Fig. 7 SS-petri model of chemical tank control system

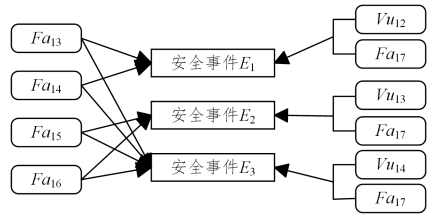


图 8 安全事件

Fig. 8 Safety events

得到 SS-petri 网模型后，根据 SS-petri 网模型进行系统级的风险分析与计算，具体如下。

(1)初始节点的风险量化

关于功能安全初始节点的风险量化，主要参照表 3 和式(11)。以 P_{10} 和 OpenPLC 机械失效为例，通过 OpenPLC 的使用手册可以得知其并未有 SIL 等级，所以 $S=0.1$。由于 PLC 在环境中一般不会有其他变动，因此不考虑其他因素。得到 $Basescore(p)=S\times A\times E\times P=0.1$。以此类推，得到其他的功能安全初始节点的量化风险并计算条件概率。

然后对信息安全初始节点进行风险量化，查阅相关 CVE 编号对应的 CVSS 分数，结合表 2 与式(11)进行。以节点 P_8 为例，CVE-2020-1938 的 base 属性为攻击向量(远程网络访问)、攻击复杂性(低)、需要权限(无)、用户交互(无)，计算得到 $Basescore(p)=8.22\times AV\times AC\times PR\times UI/10=0.39$。

(2)条件节点的局部条件概率分布计算

得到初始节点的风险量化结果后，依据式(13)和式(14)计算得出节点的条件概率值。以节点 P_{22} 为例，$Basescore(p_{22})=P_{14}\times[1-(1-P_{13})\times(1-P_{15})\times(1-P_{16})]=0.31$。以此类推，计算出所有的节点条件概率，如表 8 所列。

表 8 节点概率

Table 8 Node probability

功能安全节点	概率	信息安全节点	概率
P_1	0.001	P_5	1
P_2	0.01	P_6	1
P_3	0.2	P_7	0.28
P_4	0.1	P_8	0.39
P_{10}	0.1	P_9	0.28
P_{11}	0.29	P_10	0.2
P_{12}	0.29	P_{13}	0.56
P_{17}	0.29	P_{14}	0.39
P_{18}	0.1	P_{15}	0.2
P_{19}	0.1	P_{16}	0.28
P_{20}	0.1	P_{22}	0.31
P_{21}	0.1		
P_{30}	0.1		

(3)路径的概率计算

根据 SS-petri 网模型中的变迁 t 生成攻击路径，并根据表 8 的节点概率计算出某条路径的攻击可能性。以路径(t_1，t_7，t_{17}，t_{24})为例，$P(t_1,t_7,t_{17},t_{24})=p(t_{24}\mid t_1,t_7,t_{17})p(t_{17}\mid t_1,t_7)p(t_7\mid t_1)p(t_1)=0.31*0.56*0.39=0.07$，以此类推其他的路径攻击可能性。

对于化工罐控制系统而言，由前文的分析可知，主要的安全事件分为 3 种，分别对应现实中化工罐产品反应进行前、

反应进行中、反应结束后出现的泄露和爆炸等3类安全事件，可以依据式(16)计算对应安全事件的损失。其中，化工罐爆炸导致的人员损失参照文献[35]给出，系统的资产损失参照式(18)给出，系统信息安全损失参照标准GB/T 31509-2015[36]给出。文献[37]中对爆炸事故场景下的不同损失进行了分析，其中人员损失使用生命价值统计(VSL)进行量化，因此本文取VSL为200万元为标准进行归一化，设备经济损失与信息安全经济损失取实际值。本文依据其结果，通过不同损失之间的对比设计损失参数，取 λ_1，λ_2 和 λ_3 为0.25，0.7和0.05，安全事件的损失如下：

安全事件 E_1：$L_1=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.38$

安全事件 E_2：$L_2=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.14$

安全事件 E_3：$L_3=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.86$

最终根据式(19)和式(20)得到对应的风险值：

$$\begin{aligned}Risk&=\max\{risk_1,risk_2,risk_3\}\\&=\max\{(SP_1\times L_1),(SP_2\times L_2),(SP_3\times L_3)\}\\&=\max\{0.68\times 0.38,0.14\times 0.52,0.86\times 0.79\}\\&=0.679\end{aligned}$$

从而求得化工罐控制系统的风险值为0.679。

根据最终风险评价的要求即表4可知该系统的风险等级为中高，因此需要采取措施降低风险。

4.3 实验结果与分析

为了证明一体化风险评估的有效性与全面性，实验选择了功能安全(故障树)和信息安全(攻击树)两种风险评估代表性方法，基于相同的实验场景开展风险评估并进行对比。

基于相同的功能安全风险数据集，对系统进行故障树分析，结果如图9所示。单纯功能安全故障树分析得到的系统风险值为 $Risk=0.003$。

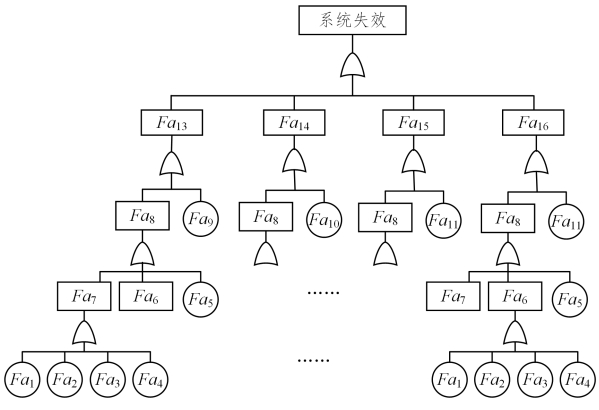


图9 故障树分析图

Fig. 9 Fault tree analysis

接着基于相同的信息安全风险数据集，对系统进行攻击树分析，结果如图10所示。单纯信息安全攻击树分析得到的系统风险值为 $Risk=0.473$。

在本文的实验环境下，单领域的风险评估难以判断PLC机械失效、PLC数据篡改、阀门失效等事件之间的关系，从而影响风险缓解措施的制定(如安全仪表设施的选择、网络防护设施的选择等)。如表9所列，基于相同的风险数据集，只考虑物理域或信息域风险的故障树或攻击树模型计算出的系风险值统分别为0.003和0.473；而本文所提方法同时考虑物理域与信息域风险，还将可能出现的信息物理协同攻击也作为一个风险点包含在内，因此计算出系统风险值为0.679，该值高于故障树和攻击树模型计算出的系统风险值，说明本文所提方法更为全面完善。

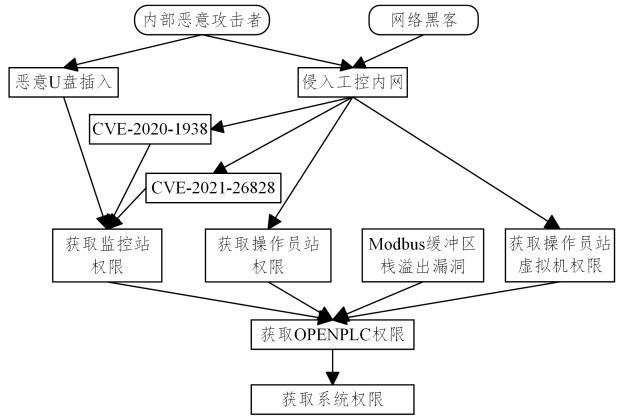


图10 攻击树分析图

Fig. 10 Attack tree analysis

表9 功能安全、信息安全与一体化安全分析对比

Table 9 Analysis comparison of functional security, information security and integrated security

方法	故障树	攻击树	SS-petri网
范围	功能安全	信息安全	一体化安全
量化标准	专家经验	信息安全数据	一体化安全数据集
对信息物理协同攻击识别	否	否	是
攻击路径的生成	否	否	是
系统风险值	0.003	0.473	0.679

值得注意的是，本文是对仿真化工罐控制系统的模拟，目的是验证所提方法的可行性，采用的数据大多来自元件手册及网络开源数据库。对于真实的大型工业控制系统环境，可以创建功能安全与信息安全一体化相关数据库(如事故数据库、组件失效数据库、漏洞库等)，或依赖专家经验进行针对性更强的初始风险量化。

结束语 本文提出了一种融合功能安全和信息安全的一体化风险评估方法SSPN-RA，包括安全一体化风险识别、一体化风险分析和一体化风险评估3个步骤。该方法从风险识别的数据入手，通过同时收集功能安全和信息安全风险数据构建风险识别数据库；接着在SS-petri网模型中分析风险识别数据并构造信息物理协同的攻击路径，通过计算由安全事件导致的功能安全损失、信息安全损失和安全事件发生概率得到风险值，在一体化风险评估方法中实现了功能安全和信息安全的融合。在仿真化工罐控制系统中对其进行实验验证，并与功能安全故障树分析方法和信息安全的攻击树分析方法两种代表性风险评估方法进行对比，从而证明本文所提方法的先进性。本文提出的风险评估方法可以分析出系统最有可能发生的安全事件并分别计算出系统中所有安全事件的风险值。

未来的研究方向包括3个方面。(1)对SS-petri网模型的改进，中小型工业控制系统的拓扑结构相对清晰明朗，能够轻易构造相应模型。但随着节点及数据的增加，SS-petri网

模型的构造存在效率低的缺陷，因此需要改进其算法使其更具有适应性。(2)文中只考虑了工业控制系统的过程控制区，该系统还包括企业资源规划区(ERP)和制造执行系统(MES)，这些区域中可能包含有关功能安全与信息安全的内容，因此需要改进计算方式，同时考虑整体的风险值。(3)工业控制系统中也存在很多网络防护工具(例如蜜罐、入侵检测系统等)及安全相关控制系统，本文并未将它们考虑在内，因此在之后的工作中也需要考虑到对工业控制系统中的防御策略的量化。

参 考 文 献

[1] WEI Q, WANG W H, CHEN P. Industrial Internet Security: Architecture and Defense [M]. China Machine Press, 2021.

[2] JIN J H, MO C Y, LI G. Integration Technology of Functional Safety and Cyber Security for Industrial Control System[J]. Industrial Safety and Environmental Protection, 2020, 46(1): 53-60.

[3] LANGNER R. Stuxnet: Dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[4] 全国工业过程测量控制和自动化标准化技术委员会. GB/T 20438-2017：电气/电子/可编程电子安全相关系统的功能安全[S]. 中国国家标准化管理委员会：中国国家标准化管理委员会，2017.

[5] 全国工业过程测量和控制标准化技术委员会，全国信息安全标准化技术委员会. GB/T 30976.1-2014：工业控制系统信息安全-第 1 部分：评估规范[S]. 中国国家标准化管理委员会：中国国家标准化管理委员会，2014.

[6] ISO technical committee 262: Risk management, IEC technical committee 56: Dependability. ISO 31010-2019: Risk management-Risk assessment techniques[S]. ISO: ISO, 2019.

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

[8] KABIR S, WALKER M, PAPADOPOULOS Y. Dynamic system safety analysis in HiP-HOPS with Petri Nets and Bayesian Networks[J]. Safety Science, 2018, 105: 55-70.

[9] 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.

[10] CUI Y, QUDDUS N, MASHUGA C V. Bayesian network and game theory risk assessment model for third-party damage to oil and gas pipelines[J]. Process Safety and Environmental Protection, 2020, 134: 178-188.

[11] MAHMOUDI J. A Four-Step Safety Integrity Level Analysis of Numerous Subsea Control System Components [J]. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, 2021, 7(3): 031005.

[12] HUANG K, ZHOU C, TIAN Y C, et al. Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks[C]// 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, 2017: 1-6.

[13] ZHANG Q, ZHOU C, 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, 2017, 14(6): 2497-2506.

[14] ZHANG Q, ZHOU C, 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, 2017, 14(6): 2497-2506.

[15] LI X, ZHOU C, TIAN Y C, et al. Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2017, 14(2): 608-618.

[16] SCHMITTNER C, GRUBER T, PUSCHNER P, et al. Security application of failure mode and effect analysis (FMEA)[C]// Computer Safety, Reliability, and Security: 33rd International Conference (SAFECOMP 2014). Springer International Publishing, 2014: 310-325.

[17] PIÈTRE-CAMBACÉDÈS L, BOUISSOU M. Cross-fertilization between safety and security engineering[J]. Reliability Engineering & System Safety, 2013, 110: 110-126.

[18] SABALIAUSKAITE G, ADEPU S. Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security[C]// 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). IEEE, 2017: 41-48.

[19] 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.

[20] FRIEDBERG I, MCLAUGHLIN K, SMITH P, et al. STPA-SafeSec: Safety and security analysis for cyber-physical systems [J]. Journal of Information Security and Applications, 2017, 34: 183-196.

[21] KRIAA S, BOUISSOU M, LAAROUCHI Y. A new safety and security risk analysis framework for industrial control systems [J]. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of risk and reliability, 2019, 233(2): 151-174.

[22] ASSANTE M J, LEE R M. The industrial control system cyber kill chain[J]. SANS Institute InfoSec Reading Room, 2015, 1: 24.

[23] RUIJTERS E, STOELINGA M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools[J]. Computer Science Review, 2015, 15: 29-62.

[24] LALLIE H S, DEBATTISTA K, BAL J. A review of attack graph and attack tree visual syntax in cyber security[J]. Computer Science Review, 2020, 35: 100219.

[25] ALAEDDINI A, DOGAN I. Using Bayesian networks for root cause analysis in statistical process control[J]. Expert Systems with Applications, 2011, 38(9): 11230-11243.

[26] KHAKZAD N, KHAN F, AMYOTTE P. Dynamic risk analysis using bow-tie approach[J]. Reliability Engineering & System Safety, 2012, 104: 36-44.

[27] Forum of Incident Response and Security Teams. Common Vul-

nerability Scoring System version 3.1: Specification Document [OL]. [2021]. https://www.first.org/cvss/specification-document.

[28] SWINBURNE R. Bayes' theorem [J]. Revue Philosophique DeLla France Et De L, 2004, 194(2): 250-251.

[29] GB/T 36466-2018, 信息安全技术工业控制系统风险评估实施指南[S]. 中国国家标准化管理委员会: 中国国家标准化管理委员会, 2018.

[30] GONG S D. Cyber Security Risk Assessment for Industrial Control System based on Analytic Hierarchy Process and Attack Graph[D]. Nanchang: Nanchang Hangkong University, 2018.

[31] FORMBY D, RAD M, BEYAH R. Lowering the barriers to industrial control system security with {GRFICS}[C]// 2018 USENIX Workshop on Advances in Security Education (ASE 18). 2018.

[32] FORTIPHYD N. Version 2 of the Graphical Realism Framework for Industrial Control Simulation (GRFICS) [OL]. https://github.com/Fortiphyd/GRFICSv2.

[33] ALVES T R, BURATTO M, DE SOUZA F M, et al. OpenPLC: An open source alternative to automation[C]// IEEE Global Humanitarian Technology Conference (GHTC 2014). IEEE, 2014: 585-589.

[34] DERAISON R, GULA R, HUFFARD J. Tenable Nessus [OL]. https://www.tenable.com/downloads/nessus.

[35] ZAREI E, KHAN F, ABBASSI R. Importance of human reliability in process operation: A critical analysis[J]. Reliability Engineering & System Safety, 2021, 211: 107607.

[36] 全国信息安全标准化技术委员会. GB/T 31509-2015: 信息安全技术信息安全风险评估实施指南[S]. 中国国家标准化管理委员会: 中国国家标准化管理委员会, 2017.

[37] FAKHRAVAR D, COZZANI V, KHAKZAD N, et al. Security vulnerability assessment of gas pipeline using Bayesian network [C]// 27th European Safety and Reliability Conference, ESREL 2017. CRC Press/Balkema-Taylor & Francis Group, 2017: 1171-1180.

MA Zigang, born in 1999, postgraduate. His main research interests include industrial security and so on.

MA Rongkuan, born in 1992, Ph.D. His main research interests include industrial security and IoT security.

(责任编辑: 柯颖)