工业控制系统功能安全和信息安全一体化风险评估方法

马叶桐[1,2], 丁云杰[1,2], 刘圃卓[1,2], 吕世超[1,2], 潘志文[1,2], 孙利民[1,2]

[1] 中国科学院大学网络空间安全学院 北京 中国 100049

[2] 中国科学院信息工程研究所 物联网信息安全技术北京市重点实验室 北京 中国 100093

摘要 信息化与工业化的深度融合打破了工业控制系统封闭的网络边界，导致传统信息系统网络攻击威胁渗透至工业控制系统网络。工业控制系统除了需要考虑传统功能安全风险外，还需要关注信息安全风险。本文提出了一种被命名为 SSRA 工业控制系统功能安全和信息安全一体化风险评估模型和算法，包括安全一体化风险数据收集、一体化风险分析和一体化风险评价三个步骤。该模型从风险数据来源的角度入手，同时收集功能安全和信息安全风险数据，在风险分析步骤中生成可分析信息物理协同攻击路径的扩展攻击树模型，对功能安全风险传播和信息安全漏洞利用难度进行量化，在计算安全事件风险时同时考虑事件导致的功能安全损失和信息安全损失等，从而实现功能安全和信息安全的一体化风险评估。本文介绍工业控制系统安全一体化风险评估模型和算法，在搭建的燃气管网测试系统中验证了本方法的有效性，并将评估结果与故障树、攻击树、攻击树与蝴蝶结结合(AT-BT)等现有风险评估方法的评估结果进行对比。实验结果表明，本文提出的安全一体化风险评估方法实现了风险评估流程的简化，不仅可以分析出系统中最有可能发生的安全事件，也在一定程度上解决了现有风险评估方法无法识别物理域与信息域相互影响情况下的安全风险问题。

关键词 功能安全；信息安全；安全一体化；风险评估；攻击树；工业控制系统

中图法分类号 TP29

Integrated Risk Assessment Algorithm for Functional Safety and Information Security of Industrial Control Systems

MA Yetong[1,2], DING Yunjie[1,2], LIU Puzhuo[1,2], LV Shichao[1,2], PAN Zhiwen[1,2], SUN Limin[1,2]

[1] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

[2] Beijing Key Laboratory of IoT Information Security Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract The deep integration of informatization and industrialization has broken the closed network boundaries of industrial control systems, leading to the penetration of traditional information system network attack threats into the industrial control system networks. Industrial control systems not only need to consider traditional functional safety risks in them, but also need to pay attention to their information security risks. This paper proposes an integrated risk assessment model and algorithm for functional safety and information security of industrial control systems which is called as SSRA. The algorithm includes three steps, safety and security integrated risk data collection, integrated risk analysis and integrated risk evaluation. This algorithm starts from the perspective of the source of risk data, collects functional safety and information security risk data at the same time. In the risk analysis step, the algorithm generates the extended attack tree model which can analysis cyber-physical coordinated attack paths, quantifies the difficulties of functional safety risk propagation and information security vulnerability exploitation, considers the functional safety loss and information security loss caused by safety events and security events when calculating event risks, etc., so as to achieve the goal of the integration of risk assessment of functional safety and information security. This paper introduces the integrated risk assessment model and algorithm for functional safety and information security of industrial control systems, verifies the effectiveness of the risk assessment algorithm in the built gas pipeline network test system, and then compares the results with the evaluation

通讯作者：吕世超, 博士, 高级工程师, Email: lvshichao@iie.ac.cn。

本课题得到国家重点研发计划(2020YFB2010902)；国家自然科学基金(No.62002342)资助。

收稿日期：201X-X-X；修改日期：201X-X-X；定稿日期：201X-X-X

results of three existing risk assessment methods, including fault tree, attack tree, the attack tree and bow-tie combination (AT-BT) method. The experimental result shows that the quantitative safety and security integration risk assessment algorithm proposed in this paper realizes the simplification of the risk assessment process, this algorithm can not only analyze the most likely safety events and security events in the system, but also solve the problem that the existing risk assessment methods cannot identify the type of safety and security risks when the physical domain and the information domain interact with each other to some extent.

Key words functional safety; information security; safety and security integration; risk assessment; attack tree; industrial control system

1 引言

工业控制系统(industrial control system, ICS)是国防军工、电力生产、石油化工、交通运输等国家基础设施的神经中枢，其安全关乎国家安全、国计民生和公共利益，是国家间网络空间对抗的首要攻击目标。

随着信息化和工业化的深度融合，为了提高工作效率，工业控制系统网络逐渐接入信息网络，打破了原来的物理封闭网络业务形态[1]。传统信息系统网络攻击威胁渗透至工业控制系统网络，这给缺乏顶层安全设计和具体安全检测防护措施的工业控制系统带来了严峻的安全问题。近年来发生的如“震网”、“Duqu”、“Flame”“Havex”等一系列重大工控安全事件证明，工业控制系统面临着严峻的信息域攻击和物理域破坏的双重风险。

为了更好的应对工业控制系统中的已知和未知安全攻击威胁，对工业控制系统进行风险评估[2]是至关重要的工作。风险评估是风险识别、风险分析和风险评估的整体过程[3]，常用的风险评估工具包括COBRA[4]、ASSET[5]、CRAMM[6]和微软评估工具[7]等。工业控制系统的风险评估包括功能安全风险评估和信息安全风险评估两个方面。二者在风险评估对象、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[8-10]所示。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[11]有：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)、故障树(fault tree, FT)等。功能安全风险的缓解方法是参考 IEC 61508[12]、IEC 62061[13]等标准进行风险定量分析后，根据安全完整性等级(safety integrity level, 简称 SIL)[12]目标制定风险缓解措施，有效减轻对人员、环境、资产、系统造成的伤害。信息安全风险评估主要分析系统面临的外部威胁，主要分析方法[11]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(具有共同安全要求的逻辑安全域或物理资产分组[14])和管道(通信资产的逻辑分组[14])，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，对资产漏洞利用的可能性及漏洞利用成功的后果进行定性分析，根据安全等级(security level, 简称 SL)[14]目标制定风险缓解措施，从而有效减少信息和资源的机密性、完整性、可用性的损失。

表 1 功能安全和信息安全风险评估的主要特点对比

Table 1 Comparison of the main features of functional safety risk assessment and information security risk assessment

	功能安全风险评估	信息安全风险评估
风险评估对象	生产过程/受控设备	生产过程区域和管道
风险来源	运行和环境的随机失效(硬件/功能失效)；	威胁：系统内/外部；脆弱性：组件/系统的设计疏漏
风险后果	对人员、环境、资产、系统造成伤害	信息和资源的机密性、完整性、可用性的损失
风险分析	一般是定量分析	一般是定性分析
参考标准	IEC 61508 等	IEC 62443 等
安全分级	安全完整性等级(SIL)	安全等级(SL)

单纯进行功能安全或信息安全的风险评估已不能满足工业控制系统安全的需求。例如只进行功能安全评估时，无法评估信息安全威胁对功能安全破坏的程度；只进行信息安全评估时，也无法衡量信息安全防护措施对系统功能安全的影响(如信息安全防护措施会增加系统通信延迟，进而降低工业控制系统业务实时性，影响系统正常业务流程，存在功能安全失效的隐患)。并且，单方面的风险评估也无法准确识别信息物理协同的高隐蔽攻击风险。此外，功能安全风险评估与信息安全风险评估在分析和评估的阶段，存在一些概念相似或内容重复的工作，二者的融合可以在一定程度上简化评估流程。

但是，由于安全一体化相关研究[15-19]没有提出合适有效的算法计算融合安全的风险值，也没有具体的模型搭建与计算公式，仅从定性分析角度出发分析系统风险，风险分析结果不够直观也难以比较，实际应用价值有限。因此，本文提出了一种功能安全和信息安全一体化风险定量评估方法，从风险数据来源的角度入手，同时识别与收集功能安全风险

和信息安全风险数据信息，并在生成的系统攻击树模型中考虑信息物理协同攻击路径，以及同时考虑安全事件导致的功能安全损失和信息安全损失等因素。本文提出的一体化风险评估方法包括一体化风险数据收集、风险分析和风险评价三个步骤。首先，在风险数据收集阶段，同时识别并收集功能安全和信息安全来源的风险数据信息；然后，在风险分析阶段，利用风险识别输出，基于扩展的攻击树模型，构建支持功能安全和信息安全一体化风险量化计算的风险评估模型；最后，在风险评价阶段，综合评价功能安全和信息安全风险等级。

本文的主要贡献包括三个方面：

1）提出一种基于攻击树模型的工业控制系统功能安全和信息安全一体化风险评估算法 SSRA(safety and security risk assessment algorithm)，实现物理域故障风险与信息域攻击威胁风险耦合影响作用的定性和定量分析。

2）将攻击树模型应用到一体化风险评估方法中来处理工业控制系统的风险源、事件、后果等相关数据，并引入贝叶斯理论解决了条件概率计算问题。

3）在搭建的燃气管网风险评估验证平台中验证提出的 SSRA 方法，实验结果表明，该方法可以有效识别、分析功能安全或信息安全单方面风险评估所不能发现的信息物理跨域风险，并分析出工业控制系统中的所有风险路径以及最有可能发生的安全事件。

2 相关工作

近年来对于工业控制系统的风险评估方法的研究，主要包括以下三个方面工作：功能安全风险评估[20-22]、信息安全风险评估[23-26]，以及功能安全和信息安全融合风险评估[15-19]。

在功能安全风险评估方面，传统的风险评估方法主要为概率风险估计(PRA)，如故障树分析(fault tree, FT)、失效模式与影响分析(failure mode effect analysis, FMEA)等。同时面对日益复杂的工控系统，贝叶斯网络和 Petri 网等方法也常常被使用。同时，考虑到工控系统本身功能安全存在极大的不确定性，模糊理论、博弈论等方法也被广泛引入功能安全风险分析当中。文献[20]将模糊理论应用于故障树分析，以解决传统故障树分析存在的历史数据不足问题；文献[21]利用贝叶斯网络和博弈论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[22]提出了基于 copula 的贝叶斯网络模型，用以解决工业控制系统中的相关变量的非线性依赖关系。

在信息安全风险评估方面，使用的风险评估方法与功能安全类似，只是将评估对象从物理域转到了信息域。文献[23]将贝叶斯攻击图(Bayesian attack graph, BAG)引入列车控制系统风险评估中，分析列车控制系统最易发生的信息安全事件并确定系统风险等级；文献[25]提出了一种基于模糊贝叶斯网络的风险评估方法，动态评估工业控制系统的信息安全风险。除此之外，文献[24]提出了数据驱动的风险评估的概念，将大数据分析与机器学习等手段引入风险评估之中。文献[26]基于集成了数据驱动的贝叶斯网络，提出了一个面向工业控制系统的信息安全风险评估框架。

在融合风险评估方面，早期工作主要为单一领域风险评估方法的拓展，文献[17]提出了 FMEAV 方法，将传统的失效模式与影响分析(FMEA)拓展为失效/威胁分析，并参考 FMEA 中的失效链的概念，提出了对威胁进行分析的威胁链及具体评判标准。文献[18]在传统的危害与可操作性分析(HAZOP)基础上添加了指导词、属性和模板，使之可以适用于信息安全场景。

单一领域方法的拓展只是实现了功能安全与信息安全的简单叠加，并未考虑二者的交互与冲突问题。部分学者基于这一现状，提出了将不同领域方法进行融合的解决方案。文献[15]将用于功能安全分析的蝴蝶结分析法(bow-tie, BT)与用于信息安全分析的攻击树分析方法(attack tree, AT)相结合，称作攻击树与蝴蝶结结合(AT-BT)方法，从而提供风险场景的完整表示，并使用化学设施中风险情景的案例研究进行证明。文献[16]提出了一种工业控制系统功能安全和信息安全联合风险分析框架 S-cube，用于监控和数据采集，基于知识库对信息物理系统的物理和功能架构进行形式化建模，自动生成包含功能安全和信息安全风险的分析结果。文献[19]将六步模型(SSM)与信息流图(IFD)相结合以实现对于工业控制系统的融合安全分析，并以新加坡 SWaT 系统为例说明了方法的适用性。

然而，上述的所有研究都没有提出合适且有效的算法计算融合安全的风险值，也没有具体的模型搭建与计算公式，仅仅是从定性分析的角度出发分析系统的融合风险，风险分析的结果不够直观也难以比较，实际应用价值有限。

本文针对相关研究工作发现的上述不足之处，提出了安全一体化的风险定量评估方法，将工业控制系统中的功能安全和信息安全进行了一体化处

理，同时识别与收集功能安全和信息安全风险数据，在攻击树模型中考虑信息物理协同攻击路径，同时考虑安全事件可能导致的功能安全损失和信息安全损失。不仅可以分析出系统中最有可能发生的安全事件，也解决了现有融合风险评估方法无法识别系统物理域与信息域相互影响类型的安全风险问题。

3 安全一体化风险评估方法

本章介绍了针对工业控制系统的功能安全和信息安全一体化的风险评估方法，包括安全一体化风险数据收集、安全一体化风险分析与安全一体化风险评价三个步骤，安全一体化风险评估方法的原理图如图 1 所示。

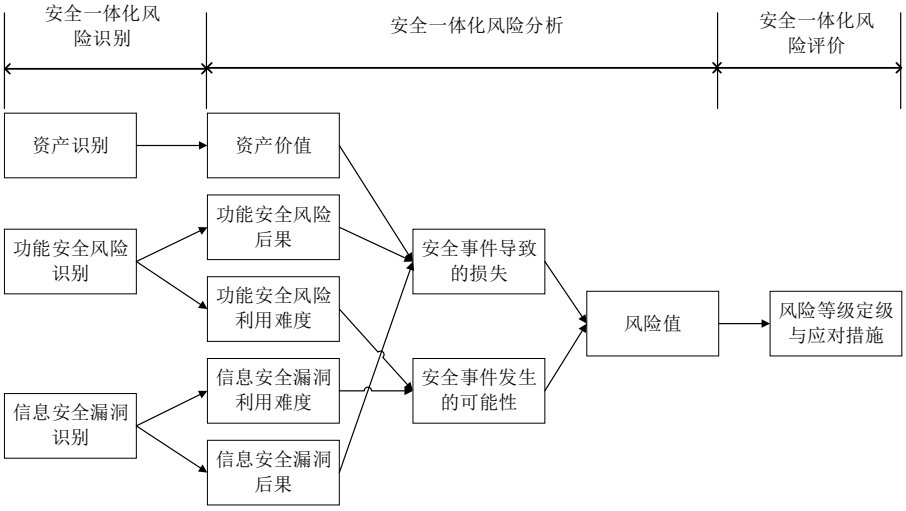


图 1 安全一体化风险评估方法原理图

Figure 1 Principle diagram of safety and security integration risk assessment method

3.1 安全一体化风险数据收集

本节主要介绍安全一体化风险评估方法的第一步：安全一体化风险数据收集，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，之后对风险数据进行形式化描述。

风险数据收集是进行风险评估的基础，可以发现、识别和描述风险。在之前的相关研究工作中，此步骤一般只收集信息安全来源的风险数据信息，而本文提出的安全一体化风险评估模型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形式化描述，从而实现了安全一体化风险数据收集。

3.1.1 风险信息的数据集来源

功能安全来源和信息安全来源的风险数据信息的数据集来源分别描述如下：

功能安全来源风险数据信息数据集主要包括：

1）对 PLC 的温度、压强、电压、湿度、防尘等物理环境要求；

2）阀门、警报器故障等机械故障；

3）人员操作失误等人为因素；

4）设备以及组件的官方手册；

5）工业生产中用到的安全检查表格等。

信息安全来源风险数据信息数据集主要包括：

1）攻击策略：ATT&CK for ICS、CAPEC 中的战术；

2）设备自身存在的信息安全漏洞：CVE、CWE 查找设备对应的漏洞编号和漏洞利用 POC 样例；

3）通信协议漏洞：设备与设备之间通信传输的漏洞；

4）人为方面的失误，例如安全意识差、使用不恰当等；

5）从 ATT&CK for ICS 等知识库收集到的信息嗅探、泄密、丢失等攻击技术等。

3.1.2 风险数据的形式化描述

收集风险数据后，对得到的风险数据进行描述。风险描述(risk description)指对风险所做的结构化的表述，通常包括风险源(指可能单独或共同引发风险的内在要素)、事件、原因和后果四个要素[27]。此步骤结果会作为风险分析步骤攻击树模型的输入。

风险描述的对象包括信息安全来源风险与功能安全来源风险两种类别，输入为 3.1.1 节所述的信息安全来源和功能安全来源的风险信息的数据集，输出则是工业控制系统中各设备组件以及设备组件之间的风险描述，具体包括：

1）资产：描述为

$$Asset=\left(id,ip,Safety\_Risk,Security\_Risk\right) \quad (1)$$

其中，*id* 表示资产的身份标识，*ip* 为资产的 IP 地址，*Safety _ Risk*,*Security _ Risk* 分别表示该资产存在的功能安全风险集和信息安全风险集，一个资产可能会有多个功能安全风险和多个信息安全风险，这些风险的集合就分别称为功能安全风险集和信息安全风险集，集合中的每个功能安全风险用功能安全风险编号表示，信息安全风险采用 CVE 等漏洞编号表示。

2）风险：指资产中存在的、可利用的不确定性对目标的影响，分为功能安全风险和信息安全风险两种，分别可以描述为

$$Safety\_Risk = (safety\_id, id, Risk\_Path) \quad (2)$$

$$Security\_Risk = (security\_id, id, Att\_rule, Att\_Stage) \quad (3)$$

其中，*safety _ id* 和 *security _ id* 分别表示功能安全风险编号和 CVE 等漏洞编号，*id* 表示功能安全或信息安全所在资产的身份标识，*Risk _ Path* 表示功能安全风险传播路径，可能包括风险源、事件和影响等要素，*Att _ Rule* 表示信息安全风险(即 CVE 等漏洞)的利用规则，*Att _ Stage* 表示该信息安全风险点位于网络攻击链(cyber kill chain)中侦查追踪、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共 7 个攻击阶段[28]中的哪个攻击阶段。

3）网络连接：指不同资产之间，通过协议建立起的传输，是网络拓扑结构的表征形式。网络的连接描述为

$$Connect = (from, protocol, to) \quad (4)$$

其中，*from*,*to* 分别表示网络连接时，数据传输的发起方、接收方，*protocol* 表示发起方与接收方两个对象之间的传输协议类型。

4）攻击者：指工业控制系统中可能会受到攻击的起点，即一条攻击路径的起始点，综合所有不同的攻击路径就会构成一棵复杂的工业控制系统攻击树。攻击者初始分布描述为

$$Attacker = (local, aip, privil) \quad (5)$$

其中，*local* 表示攻击者来源，例如外部黑客或内部恶意工作人员，*aip* 表示系统中攻击者所在的 IP 地址，*privil* 表示攻击者所具有的权限。

5）信息安全漏洞利用规则集：即资产中的信息安全漏洞的利用规则。每次原子攻击(对漏洞的一次利用过程)都需要满足一定前提条件，这些条件称为前置条件节点 C_{pre}，通常为网络中存在的漏洞、具有的某种连接关系等；一次原子攻击成功后取得目标主机的权限的节点，称为后置攻击条件节点 C_{post}，攻击后果节点通常又可以作为下一步攻击时的条件，故存在关系 $C_{post} \subset C_{pre}$。利用规则描述为

$$Att\_Rule = (security\_id, C_{pre}, C_{post}) \quad (6)$$

其中，*security _ id* 表示资产中的漏洞编号，C_{pre} 表示漏洞利用的前提条件，C_{post} 表示后置节点，即漏洞利用后的攻击后果。

6）功能安全风险传播路径集：即资产中的功能安全风险的传播路径。导致风险的要素即风险源用 R_{pre} 表示，风险事件影响目标的结果即风险后果等用 R_{post} 表示。风险源、风险事件、风险后果构成了一条功能安全风险传播链。同时，风险的后果节点通常又可以作为下一步功能安全风险事件发生时的风险源，故存在关系 $R_{post} \subset R_{pre}$。传播路径可以描述为

$$Risk\_Path = (safety\_id, R_{pre}, R_{post}) \quad (7)$$

其中，*safety _ id* 表示功能安全风险编号，R_{pre} 表示功能安全风险源，R_{post} 表示功能安全风险后果，即风险事件影响目标的结果。为了与信息安全漏洞利用规则集相对应，将 R_{pre} 和 R_{post} 也分别看作风险传播的前置条件节点和后置条件节点。

3.2 安全一体化风险分析

安全一体化风险数据收集成功后进行安全一体化的风险分析。风险分析涉及到了对风险源、事件、后果、不确定性等因素的详细考虑，从而可以理解风险性质特点和确定风险水平。风险分析分为定量分析与定性分析，常用的分析方法包括攻击树(attack tree, AT)模型[29]、贝叶斯网络、蝴蝶结(bow-tie, BT)[30]分析法、事件树分析 ETA、故障树分析 FTA、因果分析法等，风险分析步骤的结果会作为进行风险评估最后一步风险评价步骤的基础。

本文所用到的安全一体化风险分析子模型是扩展的攻击树模型，主要包括扩展攻击树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，风险数据收集步骤的输出会作为风险分析模型的输入，风险分析模型的输出则是攻击树模型与计算得到的风险水平。

安全一体化风险分析子模型通过在攻击树模型中同时考虑功能安全、信息安全事件和两者的相互影响以及在计算事件损失时同时考虑功能安全损失和信息安全损失，其中前者包括对人员、资产、环境的影响，后者包括对信息资源的机密性、完整性、可用性的影响，从而实现了风险分析过程中的安全一体化。

3.2.1 工业控制系统攻击树的生成

扩展的攻击树(attack tree, AT)是由原子攻击节点

(椭圆)、条件节点(矩形)、边和节点概率四个元素构成，可以形式化描述为四元组：

$$AT(C_{pre} \cup C_{post} \cup R_{pre} \cup R_{post}, A_{safety} \cup A_{security}, \tau, P) \quad (8)$$

式中，$C_{pre} \cup C_{post} \cup R_{pre} \cup R_{post}$ 表示攻击树的条件节点集，包括信息安全漏洞利用前置条件节点和后置条件节点，也包括了风险传播的前置条件节点和后置条件节点。A_{safety} 表示功能安全风险节点集，$A_{security}$ 表示信息安全原子攻击节点集，集合中每个元素 a_{safety} 和 $a_{security}$ 分别表示攻击者利用资产的功能安全风险进行一次风险传播或利用资产的漏洞发动一次攻击。τ 为扩展的攻击树的有向边集合，且 $\tau \subseteq (C_{pre} * A_{security}) \cup (A_{security} * C_{post}) \cup (R_{pre} * A_{safety}) \cup (A_{safety} * R_{post})$ 表示扩展的攻击树中的条件依赖关系。P 为节点的局部条件概率函数集，集合中的每个元素是 AT 每一个节点的概率分布，通常采用条件概率分布表来表示。

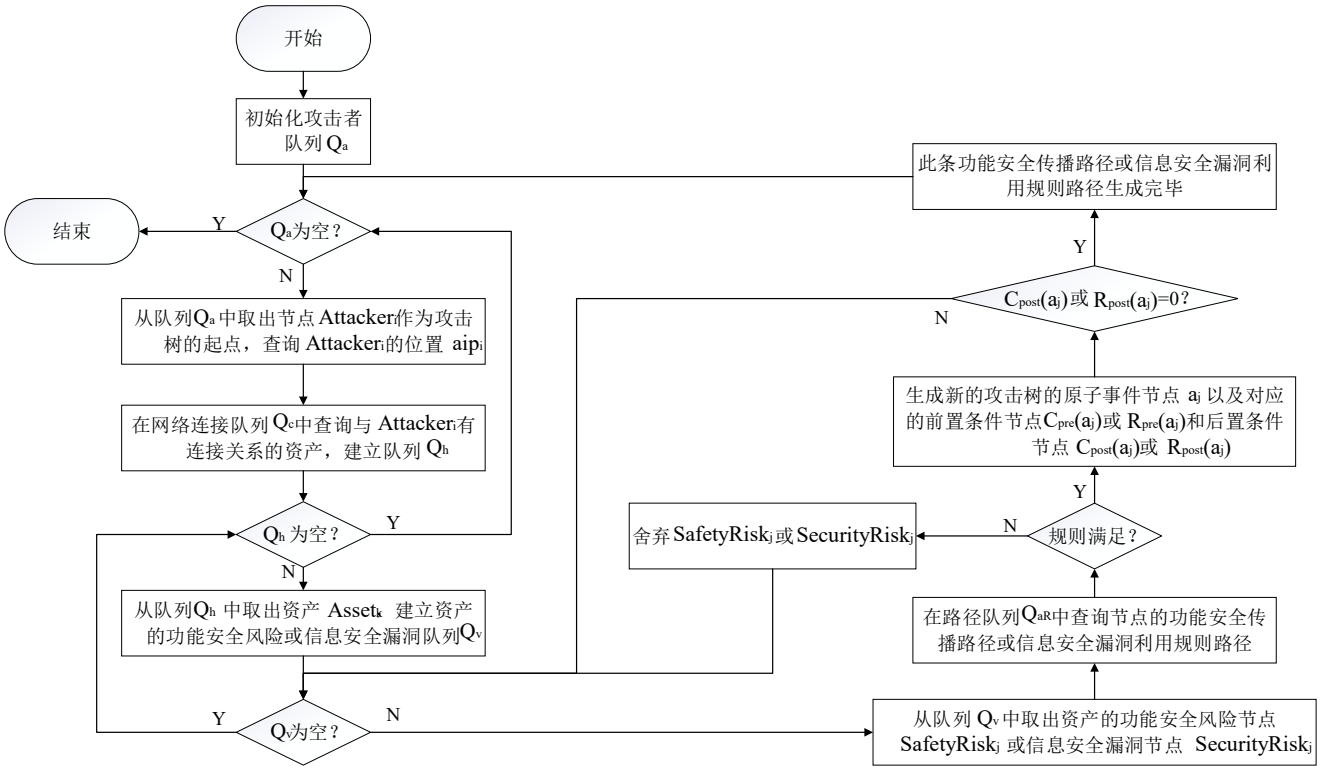


图 2 扩展攻击树的生成流程图

Figure 2 Flowchart for the generation of the extended attack tree

假设攻击行为符合单调性特征，将功能安全风险传播起点到功能安全风险传播目标节点所经过节点的组合称为功能安全风险传播路径，将信息安全漏洞利用起点到信息安全漏洞利用目标节点所经过节点的组合称为信息安全漏洞利用路径，之后将所有的功能安全风险传播路径与信息安全漏洞利用路径构成攻击树。在复杂的工业控制系统中，仅靠人力可能无法全部遍历到所有的可能路径，因此需要可以通过风险分析模型的输入自动生成扩展攻击树的算法，参考之前文献的图生成算法流程[23]，制定扩展的攻击树生成算法流程图如图 2 所示，流程说明如下：

1）分析系统的网络拓扑结构以及功能安全风险传播与信息安全漏洞利用规则信息，提取扩展攻击树的要素：网络连接 $Connect_i$ 、攻击者初始分布 $Attacker_i$ 、信息安全漏洞利用规则 Att_Rule_i 、功能安全风险传播路径 $Risk\_Path_i$，分别建立网络连接队列 Q_c 、攻击者初始分布队列 Q_a 、路径队列 Q_{aR}；

2）判断队列 Q_a 是否为空，若为空，则流程结束；否则，从队列 Q_a 中取一个元素 $Attacker_i$，作为一条攻击路径的起点，根据 $Attacker_i$ 的 IP 地址 aip_i 在 Q_c 中查询与该节点有连接关系的组件，建立队列 Q_h；

3）判断队列 Q_h 是否为空，若为空，则转向步骤 2)；否则，从队列 Q_h 中取个与 $Attacker_i$ 节点有连接关系的节点 $Asset_k$，在队列 Q_v，查询资产 $Asset_k$ 的功能安全风险或信息安全漏洞；

4）判断队列 Q_v 是否为空，若为空，则转向步骤

3）；否则，从队列 Q_v 中取功能安全风险 $Safety\_Risk_j$ 或信息安全漏洞节点 $Security\_Risk_j$，在路径库 Q_{aR} 中，查询是否满足该风险的传播路径或该脆弱性的利用规则，若不满足则舍弃，转向 4），否则生成新的攻击树原子节点 a_j，及对应的前置条件节点 $C_{Pre}(a_j)$ 或 $R_{Pre}(a_j)$ 和后置条件节点 $C_{Post}(a_j)$ 或 $R_{Post}(a_j)$；

5）判断后置节点是否为 0，若是，则该条攻击路径生成完毕，转向步骤 2）；否则，转向 4）。

具体的算法如算法 1 所示。

算法 1．扩展攻击树的生成算法。

输入：网络连接队列 Q_c、攻击者初始分布队列 Q_a、功能安全风险传播路径和信息安全漏洞利用规则路径(以下统称为路径)队列 Q_{aR}；

输出：攻击树 AT．

a) WHILE $Q_a \neq \varnothing$ do

b) $Attacker_i \in Q_a$；

$Q_h \leftarrow$ 与 $Attacker_i$ 有连接关系的资产；

c) IF $Q_h \neq \varnothing$ THEN

d) $Asset_k \in Q_h$

$Q_v \leftarrow$ 资产 $Asset_k$ 的功能安全风险节点和信息安全漏洞节点；

e) IF $Q_v \neq \varnothing$ THEN

f) $Safety\_Risk_j$ or $Security\_Risk_j \in Q_v$；

在路径队列 Q_{aR} 中查询 $Safety\_Risk_j$ 或 $Security\_Risk_j$ 的路径；

g) IF 路径 $\neq \varnothing$ THEN

h) $a_j \leftarrow Safety\_Risk_j$ 功能安全风险节点或 $Security\_Risk_j$ 信息安全漏洞节点；

$C_{Pre}(a_j)$，$C_{Post}(a_j)$ 或 $R_{Pre}(a_j)$，$R_{Post}(a_j) \leftarrow Security\_Risk_j$ 或 $Safety\_Risk_j$ 的前置和后置条件节点；

i) IF $C_{Post}(a_j)$ 或 $R_{Post}(a_j)=0$ THEN Goto ①；

j) ELSE GOTO g)；

k) ENDIF

l) ELSE

m) 删除 $Safety\_Risk_j$ 功能安全风险节点或 $Security\_Risk_j$ 信息安全漏洞节点；

GOTO g)；

n) ENDIF

o) ELSE GOTO d)；

p) ENDIF

q) ELSE GOTO a)；

3.2.2 工业控制系统级风险分析与计算

根据上述算法 1 成功生成扩展攻击树之后，接着就是对得到的扩展攻击树进行系统级的风险分析与计算，具体包括以下三个子步骤：

1）对攻击树的原子节点的攻击难度的量化。

对攻击树的原子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风险或信息安全漏洞对攻击树的原子节点进行一次功能安全风险的传播或进行一次信息安全漏洞的利用的难易程度的量化，因此原子节点攻击难度应从信息安全漏洞利用难度与功能安全风险传播难度两种情况进行考虑。

首先考虑信息安全漏洞利用难度的量化指标。通用漏洞评分系统(common vulnerability scoring system, CVSS)是一个公开标准框架，常用于测评量化漏洞的特征和严重程度，包括 Base、Temporal 和 Environmental 三个属性。Base 代表随时间和跨用户环境保持不变的漏洞本身的基本属性，Temporal 反映随时间变化的漏洞特征，Environment 代表用户环境所特有的漏洞特征，三个属性会用到不同的要素以及打分计算公式。Base 度量标准组得出一个值在 0 到 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[31]。

Base 属性包含可利用性指标(exploitability metrics)、影响指标(impact metrics)和范围(scope)三个部分，如图 3 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(privileges required, PR)，用户交互(user interaction, UI)等要素。本文选择上述四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。

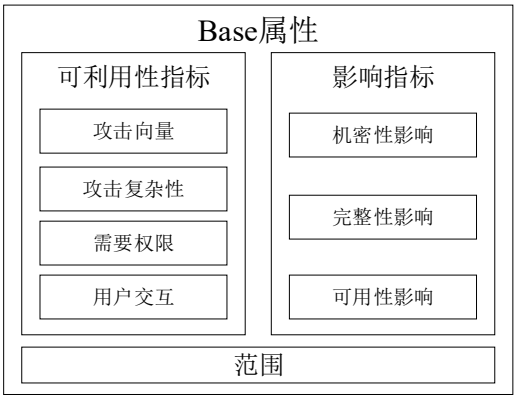


图 3 Base 属性包含的要素

Figure 3 Elements included in the Base property

如下表 2 所示，CVSS 将这四个要素划分为不同的等级，并进行相应的数值量化[31]。

表 2 可利用指标中的四个要素的等级描述与数值量化

Table 2 Level descriptions and numerical quantification of the four elements of the available indicators

要素	要素等级描述	数值量化
攻击向量	物理访问	0.2
	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	高	0.44
	低	0.77
需要权限	高	0.27
	低	0.62
	无	0.85
用户交互	需要	0.62
	无	0.85

本文参考 CVSS 的分数计算过程[31]，提出下式计算信息安全漏洞利用难度的值，并进行归一化[32]：

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

式中，AV,AC,PR,UI 分别为攻击树中的信息安全原子事件节点 a 的 Base 属性中要素 AV、AC、PR、UI 的等级的量化数值，$BaseScore(a)$ 即为信息安全原子事件节点 a 的攻击难度。

接着参考信息安全漏洞利用难度的量化指标以及 CVSS 量化思路，列出功能安全风险传播难度量化的四项指标，对此四个指标进行等级描述与数值量化如表 3 所示。

表 3 功能安全的四个要素的等级描述与数值量化

Table 3 Level descriptions and numerical quantification of the four elements of functional safety

要素	要素等级描述	数值量化
SIL 等级(S)	无	1
	SIL1	0.1
	SIL2	0.01
	SIL3	0.001
	SIL4	0.0001
事故数据(A)	无	1
	高	0.1
	中	0.01
	低	0.001
通用可靠性数据(R)	无	1
	高	0.1
	中	0.01
	低	0.001
人因错误(P)	无	1
	高	0.8
	中	0.2
	低	0.01

参考表 3 与信息安全漏洞利用难度计算公式，提出功能安全风险传播难度的值计算式如下：

$$BaseScore(a)=S\times A\times R\times P \tag{10}$$

式中，S,A,R,P 分别为攻击树中的功能安全原子事件节点 a 的要素 SIL 等级、事故数据、通用可靠性数据、人因错误的等级的量化数值。$BaseScore(a)$ 即为功能安全原子事件节点 a 的攻击难度。

因此，综合两种情况可以得到攻击树的原子节点的攻击难度计算如下：

$$BaseScore(A)=\begin{cases}\dfrac{8.22\times AV\times AC\times PR\times UI}{10}, A\in \mathrm{Sec}urity\_Risk\\ S\times A\times R\times P, A\in Safety\_Risk\end{cases} \tag{11}$$

2）条件节点和原子攻击节点的局部条件概率分布计算。

对攻击树原子节点的攻击难度成功量化之后，接着进行节点的局部条件概率分布的计算，包括对条件节点和原子攻击节点两类节点的局部条件概率的分布计算。

先看第一类条件节点，引入贝叶斯定理[33]，给出条件节点 c 为 true 的局部条件概率计算如下式：

$$P(c=true\mid F[c])=\begin{cases}P(c), F[c]=\varnothing\\ 0, F[c]\neq\varnothing, \forall a_i\in F[c], a_i=false\\ 1-\prod\limits_{a_i\in F[c], a_i=true}(1-P(c=true\mid a_i=true)), otherwise\end{cases} \tag{12}$$

其中，c 为攻击树的条件节点，a 为原子攻击节点，$F[c]$ 为 c 的父节点。父节点 $F[c]=\varnothing$，表示该节点为初始条件节点，反之则为非初始条件节点。非初始条件节点的父节点的原子攻击 $a_i=false$ 时，也即没有利用 a_i 发动攻击，节点 c 的事件不会发生，即 $P(c=true\mid F[c])=0$。除了上述两种情况外，指向条件节点的多个原子节点存在着“OR”的关系，故可求得节点概率如式中 otherwise 情况对应的公式所示。

接着看第二类原子攻击节点。对于原子攻击节点来说，只有当所有前提攻击条件满足的情况下，原子攻击才有可能发生，而不是必定发生。但当原子攻击的前提条件有一个不满足时，则原子攻击必定不会发生。原子攻击节点的条件存在“与”的关系，故原子攻击节点 a 的局部条件概率分布函数为

$$P(a=true\mid C_{\mathrm{Pre}}(a))=\begin{cases}0, \exists c_i\in C_{\mathrm{Pre}}(a), c_j=false\\ BaseScore(a), otherwise\end{cases} \tag{13}$$

式中，a 表示原子攻击节点，c 表示条件节点，$BaseScore(a)$ 为原子攻击难度，$C_{\mathrm{Pre}}(a)$ 表示 a 的前置条件节点。

3）功能安全风险传播路径或信息安全漏洞利用规则路径的风险值计算。

功能安全风险传播路径和信息安全漏洞利用规则路径的风险值应该与其发生的可能性和其对工业控制系统的影响两个因素相关，下面分别对这两个因素进行分析。

首先对事件发生的可能性进行计算。已知工业控制系统的扩展的攻击树模型中某条路径(功能安全风险传播路径和信息安全漏洞利用规则路径的总称)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[33]，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 计算如下式：

$$P = P(x_1, x_{2,...,} x_k) = p(x_k \mid x_1, x_{2,...,} x_{k-1})...p(x_2 \mid x_1)p(x_1) \quad (14)$$

式中，k 表示攻击树节点，x_k 表示节点 k 代表的随机变量。

假设攻击树原子节点事件由 $k(k \geq 1)$ 条路径并结合某种功能安全风险传播方式或信息安全漏洞利用方式引起的，则事件发生的概率 SP 计算如下式：

$$SP = \prod_{i=1}^{k} P_i \times \beta_i \quad (15)$$

式中，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，选取某种功能安全风险传播方式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，接下来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 $\lambda_1, \lambda_2, \lambda_3$ 三个变量，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 计算如下式：

$$L = \lambda_1 I_a + \lambda_2 I_p + \lambda_3 I_s \quad (16)$$

式中，$\lambda_1, \lambda_2, \lambda_3$ 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，由下式求得：

$$I_a = a_1 \times \frac{N_1}{N} + a_2 \times \frac{N_2}{N} \quad (17)$$

其中，I_a 表示资产的重要度，N_1, 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, a_2 为相对应的加权系数。

因此，事件风险值的计算如下式：

$$risk_n = SP_n \times L_n \quad (18)$$

式中，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指标，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，如下式：

$$Risk = \max\{risk_1, risk_2, ...risk_n\} \quad (19)$$

式中，$risk_i$ 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工业控制系统的扩展攻击树模型与根据此模型计算得出的工业控制系统风险值 $Risk$ 。

3.3 安全一体化风险评价

本节主要介绍安全一体化风险评估模型的最后一步——安全一体化风险评价，首先进行风险的等级划分，之后根据风险的等级采取不同的行动。

在风险分析步骤成功得出工业控制系统风险值 $Risk$ 之后，进行风险评价步骤。风险评价步骤以之前的两个步骤风险数据收集与风险分析为基础，根据风险分析步骤得出的工业控制系统风险值 $Risk$ ，得出系统发生风险的可能性以及影响程度，确定系统的风险等级，同时决策是否需要采取控制措施以及控制程度等问题。需要注意的是，工业控制系统是持续不断运行的，收集到的风险数据可能会发生变化，因此整个风险评估过程不是一次性的，而是需要通过实际工业控制系统中的风险变化，不断地进行跟踪、调整与改进。

根据文献[34]对风险进行等级划分，如表 4 所示：

表 4 风险等级划分

Table 4 Ranking of risks

风险值范围	风险等级
$0 < Risk \leq 0.2$	低
$0.2 < Risk \leq 0.4$	中低
$0.4 < Risk \leq 0.6$	中
$0.6 < Risk \leq 0.8$	中高
$0.8 < Risk \leq 1.0$	高

表 5 不同的风险等级对应的行动要求

Table 5 Action requirements corresponded to different risk levels

风险等级	行动要求
低	无需采取行动
中低	可选择(评估方案)
中	可选择(评估方案)
中高	采取行动(通知公司)
高	立即采取行动(通知公司)

将系统的风险值 $Risk$ 与表中的数值进行比对，判定工业控制系统的风险等级，从而判断此工业控制系统是否处于安全状态，决策出需要采取何种应对措施。参考《智能制造基础共性标准研究成果(三)》

[8]中的叙述，列出不同的风险等级对应的不同的行动要求，如表 5 所示。

4 实验与结果

本章主要是依据第二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燃气管网测试系统中对其进行完整的风险评估流程，从而验证安全一体化风险评估方法的可行性。首先是对实验环境即燃气管网测试系统的介绍，之后对实验完整过程进行描述，最后通过与攻击树与蝴蝶结结合(AT-BT)方法的对比对实验得到的结果进行分析。

4.1 实验环境

本节对实验环境即燃气管网测试系统进行介绍，首先介绍系统的拓扑结构，之后介绍系统的物理结构与工艺流程等。

燃气管网测试系统信息域包含两台计算机，两个 PLC，一个交换机及两个 HMI 设备。其中，设备 01 模拟操作员站，设备 02 模拟监控站，虚拟机 08 提供组态软件支持。

燃气管网测试系统物理域则主要包括 4 组传感器模块及三个电磁切断阀，其中西门子 PLC 控制高压截止阀和中压截止阀，施耐德 PLC 控制低压截止阀。

燃气管网测试系统的拓扑结构如图 4 所示，详细资产表单如表 6 所示。

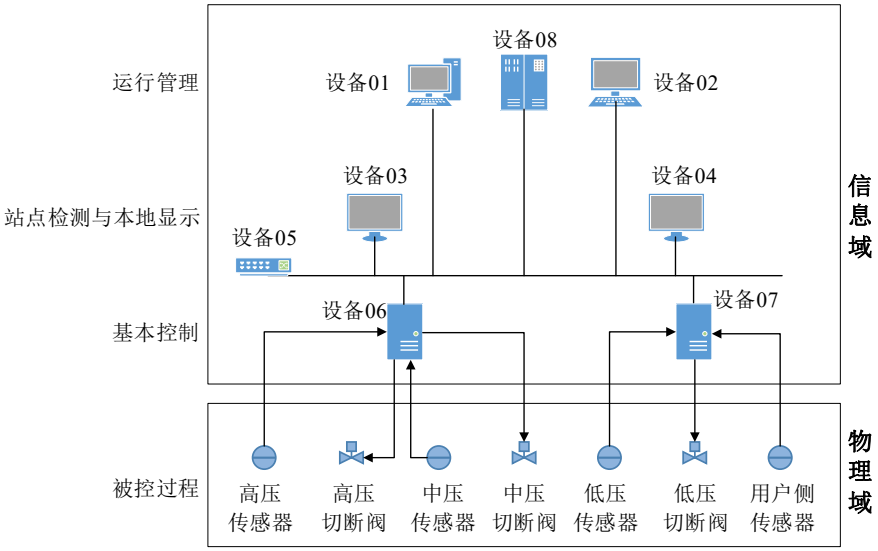


图 4 燃气管网测试系统拓扑图

Figure 4 Topology diagram of gas pipe network test system

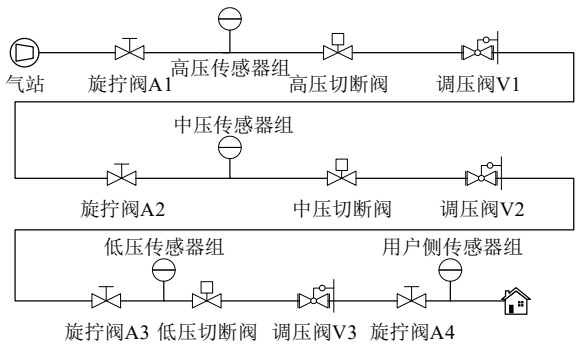


图 5 燃气管网测试系统物理结构图

Figure 5 Physical structure diagram of gas pipe network test system

燃气管网测试系统的物理结构图如图 5 所示，由一个气泵、三个调压阀、三个电磁切断阀以及四组传感器组成，其中每组传感器包括多个温度、压力、流量传感器。系统正常运行工作时的工艺流程为：首先打开气泵，模拟上游气站送气，接着气体经过三个调压阀，气压实现从高压到中压再到低压的变化，最后将居民可使用的燃气输送至用户负载。

当管道损坏产生泄露时(通过四个旋拧阀模拟)，系统通过传感器组探测到泄露发生，应当第一时间自动关闭距离泄漏点最近的两个切断阀，以预防可能发生的燃爆事件。同时，当泄露被修复时，自动打开切断阀。

燃气管网测试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 E1：当气站附近发生泄露(通过旋拧阀 A1 模拟)，高压切断阀未正常关闭；

安全事件 E2：当高压切断阀与中压切断阀间发生泄露(通过旋拧阀 A2 模拟)，高压切断阀与中压切断阀之一未正常关闭；

安全事件 E3：当中压切断阀与低压切断阀间发生泄露(通过旋拧阀 A3 模拟)，中压切断阀与低压切断阀之一未正常关闭；

安全事件 E4：当用户负载附近发生泄露(通过旋拧阀 A4 模拟)，低压切断阀未正常关闭。

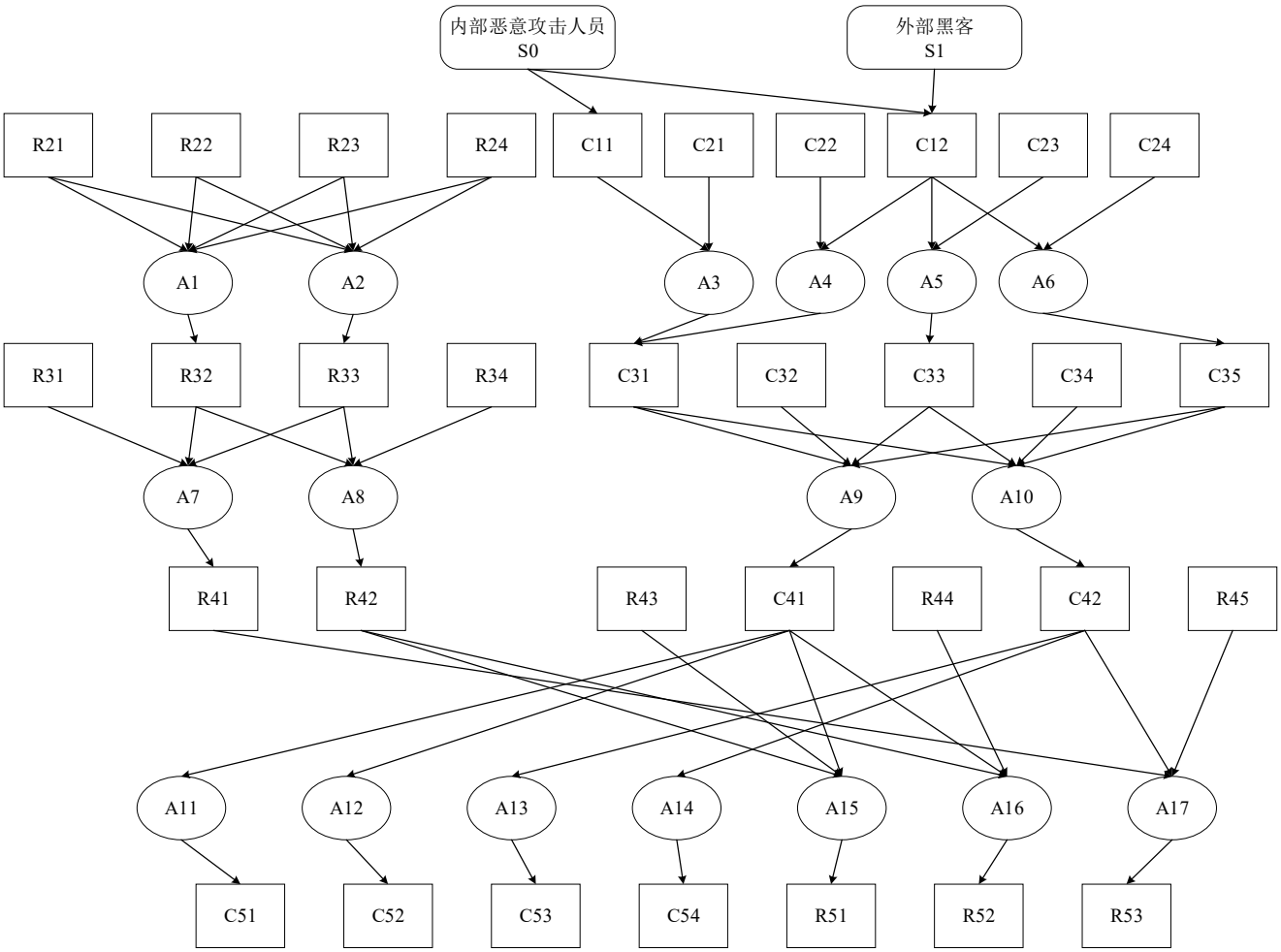


图 6 燃气管网系统攻击树

Figure 6 Attack tree of gas pipeline network system

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集主要包括：

1）eMARS 数据库[35]；

2）OREDA 数据库[36] ；

3）CORE-DATA 数据库[37] ；

4）系统元器件参数手册；

5）系统运行手册。

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[38]等资产探查扫描工具对系统的资产进行确认；

2）利用开源 OVAL 漏洞扫描器 openvas[39]对系统扫描后得到的漏洞识别结果；

3）网络攻击链(Cyber Kill Chain)[28]。

依据风险发现、识别与收集的结果，随后给出系统的风险描述，分别包括系统资产 asset 表(如表 6 所示)，系统功能安全风险表(如表 7 所示)，系统信息安全风险表(如表 8 所示)，系统风险传播路径集(如表 9 所示)。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。

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(表 6-表 9)，结合图 2 所示的扩展攻击树的生成算法，生成燃气管网测试系统攻击树如图 6 所示，燃气管网测试系统安全事件对应节点如图 7 所示。

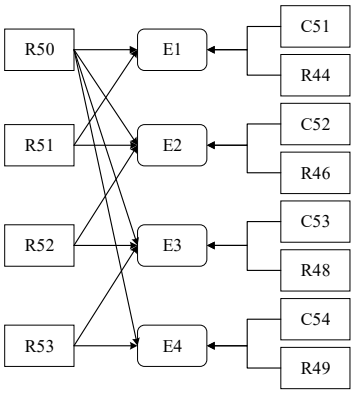


图 7 燃气管网系统安全事件

Figure 7 Safety events of gas pipeline network system

表 6 燃气管网测试系统资产列表

Table 6 Asset list of gas pipe network test system

资产 id	资产 ip 地址	资产设备描述
01	192.168.1.102	联想 Thinkcenter8500
02	192.168.1.11	联想 Thinkcenter8500
03	192.168.1.12	研华触摸屏
04	192.168.1.14	研华触摸屏
05	192.168.1.1	交换机 EDS-408A
06	192.168.1.3	西门子 S7-300
07	192.168.1.6	施耐德 Quantum3110
08	192.168.1.4	Windows xp 虚拟机

表 7 系统功能安全风险表

Table 7 Safety risk list of gas pipe network test system

Safety_id	id	备注
R21	01∪02	温度异常
R22	01∪02	断电
R23	01∪02	人员误操作
R24	01∪02	机器失效
R31	07	施耐德 PLC 机械失效
R32	02	监控站机器失效
R33	01	操作员站机器失效
R34	06	西门子 PLC 机器失效
R41	07	施耐德 PLC 失效
R42	06	西门子 PLC 失效
R43		高压截止阀机械失效
R44		高压传感器组失效
R45		中压截止阀机械失效
R46		中压传感器组失效
R47		低压截止阀机械失效
R48		低压传感器组失效
R49		用户侧传感器组失效
R51		高压截止阀失效
R52		中压截止阀失效
R53		低压截止阀失效

表 8 系统信息安全风险表

Table 8 Security risk list of gas pipe network test system

Security_id	id	Att_stage	备注
C11		载荷投递	恶意 U 盘插入
C12		载荷投递	侵入 GPNS 内网
C21	02	漏洞利用	CVE-2017-8464
C22	02	漏洞利用	CVE-2019-0708
C23	01	漏洞利用	CVE-2017-0143
C24	08	漏洞利用	SNMP NetDBServer 栈溢出漏洞
C31	02	持续控制	获取监控站权限
C32	06	漏洞利用	CVE-2015-2177
C33	01	持续控制	获取操作员站权限
C34	07	漏洞利用	Modbus 协议 0x5A 漏洞
C35	08	持续控制	获取操作员站虚拟机权限
C41	06	持续控制	获取西门子 PLC 权限
C42	07	持续控制	获取施耐德 PLC 权限
C51	06	目标达成	篡改高压传感器组数据
C52	06	目标达成	篡改中压传感器组数据
C53	07	目标达成	篡改低压传感器组数据
C54	07	目标达成	篡改用户侧传感器组数据

表 9 系统风险传播路径集

Table 9 The set of risk propagation paths of gas pipe network test system

$A_{safety} \cup A_{security}$	$C_{pre} \cup R_{pre}$	$C_{post} \cup R_{post}$
A1	R21∪R22∪R23	R32
A2	R21∪R22∪R23	R33
A3	C11∩C21	C31
A4	C12∩C22	C31
A5	C12∩C23	C33
A6	C12∩C24	C35
A7	R31∪R32∪R33	R41
A8	R32∪R33∪R34	R42
A9	C32∩(C31∪C33∪C35)	C41
A10	C34∩(C31∪C33∪C35)	C42
A11	C41	C51
A12	C41	C52
A13	C42	C53
A14	C42	C54
A15	R42∪R43∪C41	R51
A16	R42∪R44∪C41	R52
A17	R41∪R45∪C42	R53

得到攻击树模型后，下一步结合攻击树模型进行系统级的风险分析与计算，具体如下：

1）初始风险节点的风险量化

首先对功能安全初始节点进行风险量化，这一步主要参照表 3 和公式(11)。以节点 R34 为例，查阅西门子 S7-300 技术手册可得确认安全功能型 S7-300 的 SIL 等级为 3，则 S=0.001，对于单个实验环境 PLC 不考虑事故及人因要素，得到 $BaseScore(a)=S\times A\times R\times P=0.001$。以此类推得到所有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 与公式(11)进行。以节点 C22 为例，CVE-2019-0708 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 $BaseScore(A)=\dfrac{8.22\times AV\times AC\times PR\times UI}{10}=0.39$。以此类推得到所有的信息安全初始节点的量化风险并计算条件概率。

2）条件节点和原子攻击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，依据公式(12)和(13)计算得出节点的条件概率值。以节点 A9 为例，$P(c41=true\,|\,F[c])=P_{C32}\times[1-(1-P_{C31})\times(1-P_{C33})\times(1-P_{C35})]=0.21$，以此类推计算出所有的节点条件概率，如表 10 所示：

表 10 节点条件概率表

Table 10 Conditional probability table for nodes

原子节点	概率	原子节点	概率
R21	0.001	C11	1
R22	0.01	C12	1
R23	0.2	C21	0.28
R24	0.1	C22	0.39
R31	0.01	C23	0.22
R32	0.29	C24	0.28
R33	0.29	C31	0.56
R34	0.001	C32	0.28
R41	0.29	C33	0.22
R42	0.29	C34	0.28
R43	0.1	C35	0.28
R44	0.1	C41	0.21
R45	0.1	C42	0.21
R46	0.1	R47	0.001
R48	0.001	R46	0.001

3）条件节点和原子攻击节点的局部条件概率分布计算

依据表 9 提供的风险传播路径及表 10 提供的节点条件概率，可以参照公式(14)，分别计算出每条路径的可能性。以路径 $P(S_0,A_3,A_9,A_{12})$ 为例，$P(S_0,A_3,A_9,A_{12})=p(A_{12}\,|\,A_9,A_3,S_0)p(A_9\,|\,A_3,S_0)p(A_3\,|\,S_0)=0.08$,以此类推得到所有的攻击路径的可能性。

对于燃气管网测试系统而言，经前文的分析可知，主要的安全事件分为四种，分别对应现实中气站附近、变送站、郊区、市区的燃气泄漏安全事件，可以依据公式(16)计算对应安全事件的损失。其中，燃气爆炸导致的人员损失参照文献[40]给出，系统的资产损失参照公式(17)给出，系统信息安全损失参照标准 GB/T 31509-2015[41]给出。文献[42]中对实际燃气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，取 VSL 为 350W 欧元，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 $\lambda_1=0.05$，$\lambda_1=0.9$，$\lambda_1=0.05$。最终计算的安全事件对应损失如下：

安全事件 E1：$L_1=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.41$

安全事件 E2：$L_2=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.48$

安全事件 E3：$L_3=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.07$

安全事件 E4：$L_4=\lambda_1 I_a+\lambda_2 I_p+\lambda_3 I_s=0.93$

最终依据公式(18)和公式(19)计算可得对应的风险值，得到：

$$\begin{aligned}Risk&=\max\{risk_1,risk_2,risk_3,risk_4\}\\&=\max\{SP_1\times L_1,SP_2\times L_2,SP_3\times L_3,SP_4\times L_4\}\\&=\max\{0.55\times 0.41,0.48\times 0.76,0.07\times 0.78,0.93\times 0.5\}\\&=0.465\end{aligned}$$

最终求出工业控制系统的风险值 *Risk* 为 0.465。

4.3 实验结果与分析

依据风险分析得到的结果，对燃气管网测试系统开展融合风险评价。系统的最终风险值为 0.465，依据表 3 可得系统的风险等级为中，对应的行动要求为“可选择”。

为了证明一体化风险评估的有效性与全面性，本实验选择了包括功能安全(故障树)、信息安全(攻击树)和攻击树与蝴蝶结结合(AT-BT)方法共三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，得到的结果如下所示。

首先基于相同的功能安全风险数据集，对系统进行故障树分析，得到结果如图 8 所示。单纯功能安全故障树分析得到的系统风险值为：$Risk=P_{\max}L_{\max}=0.06$。

接着基于相同的信息安全风险数据集，对于系统进行攻击树分析，得到结果如图 9 所示。单纯信息安全攻击树分析得到的系统风险值为：$Risk=P_{\max}L_{\max}=0.3$。

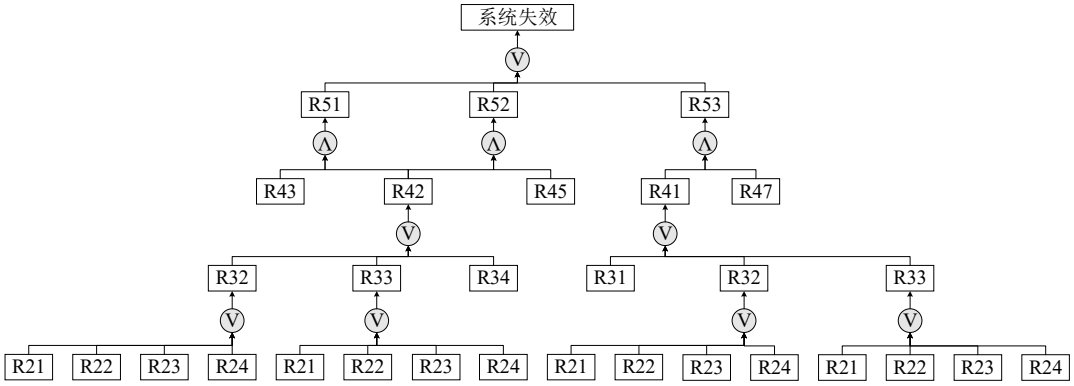


图 8 燃气管网系统故障树

Figure 8 Fault tree of gas pipeline network system

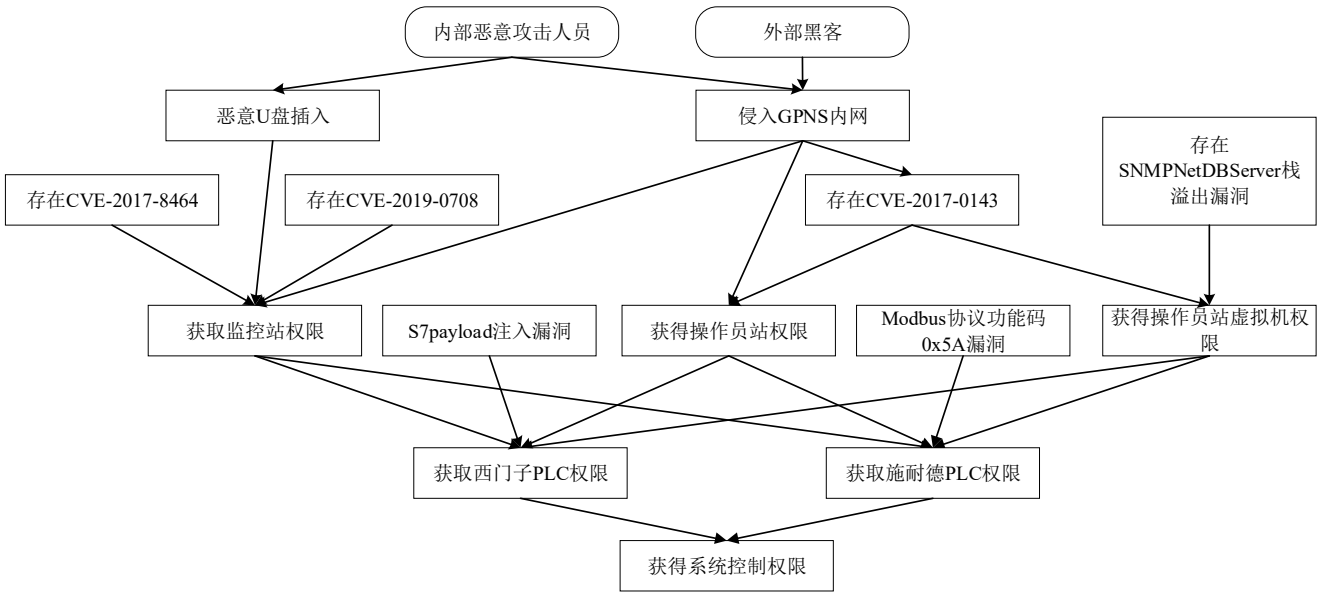


图 9 燃气管网系统攻击树

Figure 9 Attack tree of gas pipeline network system

攻击树与蝴蝶结结合(AT-BT)的分析方法是一种定性分析方法，采用风险矩阵等定级方法来描述系统风险，对于风险点的可能性评估也缺乏一致性指标，而来源于专家经验。

与上述方法相比，本文提出的安全一体化风险评估方法对工业控制系统面临的风险进行了定量分析，能够更加直观的表述描述不同风险之间的差异，同时基于贝叶斯理论，分析路径概率与事件后果，可以给出系统面临的最大威胁路径，对于下一步制定风险缓解措施提供依据。同时，如图 10 所示，现代工业控制系统可能面临着复杂的信息物理协同攻击，攻击者可能通过物理域攻击(如第三方攻击破坏管道)结合信息域攻击(如篡改传感器数据)的方式对工业控制系统造成严重损失，单纯的信息安全风险评估或功能安全风险评估无法准确识别系统面临的全部危害以及危害后果，从而影响风险缓解措施的制定。

在本文的实验环境下，单领域的风险评估难以判断传感器机械失效、传感器数据篡改、阀门失效等事件间的关系，影响风险缓解措施的制定(如不同型号传感器的选择、安全仪表设施的选择、网络防护设施的选择等)。系统风险值代表系统风险事件的后果和可能性的乘积，如表 11 所示，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统风险值分别为 0.06 和 0.3，考虑物理域和信息域风险的 AT-BT 方法属于定性分析方法，且没有考虑信息物理协同攻击的情况，而本文提出的一体化风险评估方法不仅考虑了物理域

和信息域风险，还考虑到了信息物理协同攻击，故而计算出系统风险值为 0.465，该值略高于故障树和攻击树模型计算出的系统风险值，体现出本文提出的风险评估方法更为全面完善。对于工控系统而言，故障树和攻击树分析由不同的部门进行，却存在一些概念相似或者内容重复的工作，使用一体化风险评估方法可同时实现对二者的代替，省去了一部分重叠工作，从而实现风险评估流程的简化。

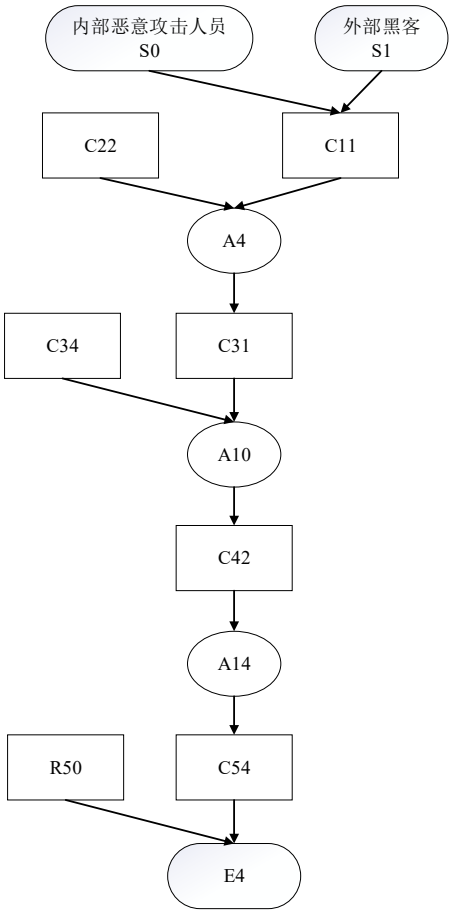


图 10 燃气管网系统威胁路径

Figure 10 Threat path of gas pipeline network system

表 11 方法对比

Table 11 Method comparison

方法	故障树	攻击树	AT-BT	一体化风险评估
覆盖范围	功能安全	信息安全	一体化安全	一体化安全
风险量化标准	专家经验	历史数据	专家经验	一体化量化标准
信息-物理协同攻击识别	否	否	否	是
系统最大威胁路径	否	否	否	是
系统风险值	0.06	0.3	定性分析	0.465

值得注意的是，本实验的环境是对真实燃气管网系统的模拟，旨在验证本文提出的安全一体化风险评估方法的可行性，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，可以建立自己的数据库(如事故数据库、维修数据库等)，或依赖专家经验进行针对性更强的初始风险量化。

5 结论

本文提出了一种工业控制系统中的功能安全和信息安全的一体化风险评估方法，包括安全一体化风险数据收集、风险分析和风险评价三个步骤。该方法从风险数据来源的角度入手，通过同时收集功能安全和信息安全风险数据、在攻击树模型中考虑信息物理协同攻击路径以及同时考虑安全事件可能导致的功能安全损失和信息安全损失等，在风险评估方法中实现了功能安全和信息安全的融合。该方法可以分析得到工业控制系统中所有可能的功能安全事件、信息安全事件和信息物理协同安全事件，并计算出系统中最有可能发生的安全事件及其风险值。本文在燃气管网测试系统中对其进行实验验证，并与包括功能安全(故障树)、信息安全(攻击树)和攻击树与蝴蝶结结合(AT-BT)方法共三种风险评估代表性方法进行对比从而分析本文提出的方法的先进性，后者可以分析出前者分析不出的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。

未来工作的可能研究方向包括三个方面。一是攻击树模型的优化与攻击树生成算法的优化，本文中的扩展攻击树模型对小型系统的适应性良好，但大型系统生成的攻击树会较为复杂，生成算法的时间和空间复杂度较高、效率较低，需要对攻击树模型及其生成算法进行优化。二是计算系统风险时，将工业控制系统风险取值为系统最有可能发生的事件有些片面，不太适应面对系统中存在两个甚至数个风险值高且风险值相近的安全事件的情况，需要优化系统的最终风险值公式以增强其普适性。三是计算系统风险时没有考虑通信管道的风险，只考虑了安全区的风险，需要同时考虑工业控制系统中的分区和子系统以及子系统之间的通信管道的风险值，并依据其相互之间的关系给出整个工业控制系统风险值的计算公式。

参考文献

[1] JIN Jianghong, MO Changyu, LI Gang. Integration Technology of Functional Safety and Cyber Security for Industrial Control System[J]. *Industrial Safety and Environmental Protection*,

2020,46(1):53-60 (in Chinese)
（靳江红,莫昌瑜,李刚.工业控制系统功能安全与信息安全一体化防护措施研究[J].工业安全与环保,2020,46(01):53-60）

[2] ISO Technical Management Board Working Group on risk management. ISO GUIDE 73-2009: Risk management-Vocabulary[S]. ISO: ISO, 2009

[3] ISO/TC 262 Risk management. ISO 31000-2018: Risk management - Guidelines[S]. ISO: ISO, 2018

[4] 2021 C&A Security Risk Analysis Group. INTRODUCTION TO COBRA [OL]. [2021]. https://security-risk-analysis.com/introduction-to-cobra/

[5] Swanson, M., Fabius, J., Stevens, M., et al. Automated Security Self-Evaluation Tool (ASSET) [OL]. [2021]. https://www.nist.gov/publications/automated-security-self-evaluation-tool-asset

[6] European Union Agency for Cybersecurity. Cramm [OL]. [2021]. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[7] Microsoft 2021. Download Microsoft Security Assessment Tool 4.0 from Official Microsoft Download Center [OL]. [2021]. https://www.microsoft.com/en-us/download/details.aspx?id=12273

[8] 国家智能制造标准化总体组. 智能制造基础共性标准研究成果（三）[M]. 北京：电子工业出版社，2020.10.

[9] SAC/TC 124. GB/T 20438-2017: Functional safety of electrical/ electronic/ programmable electronic safety-related systems[S]. Standardization Administration: Standardization Administration, 2017 (in Chinese)
（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）

[10] SAC/TC 124, SAC/TC 260. GB/T 30976.1-2014: Industrial control system security - Part 1: Assessment specification [S]. Standardization Administration: Standardization Administration, 2014 (in Chinese)
（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）

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

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

[13] IEC/TC 44. IEC 62061-2021: Safety of machinery-Functional safety of safety-related control systems[S]. IEC: IEC, 2021

[14] IEC/TC 65. IEC/TS 62443-1-2009: Industrial communication networks-Network and system security-Part 1: Terminology, concepts and models[S]. IEC: IEC, 2009

[15] 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

[16] 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

[17] Schmittner C, Gruber T, Puschner P, et al. Security application of failure mode and effect analysis (FMEA)[C]//International Conference on Computer Safety, Reliability, and Security. Springer, Cham, 2014: 310-325.

[18] Piètre-Cambacédès L, Bouissou M. Cross-fertilization between safety and security engineering[J]. Reliability Engineering & System Safety, 2013, 110: 110-126.

[19] 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.

[20] 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.

[21] 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.

[22] Guo C, Khan F, Imtiaz S. Copula-based Bayesian network model for process system risk assessment[J]. *Process Safety and Environmental Protection*, 2019, 123: 317-326.

[23] Kuang Xiangqi. Research on Risk Assessment Method of Information Security in Communication-Based Train Control Systems[D]. Beijing Jiaotong University, 2018 (in Chinese)
（邝香琦. CBTC 系统信息安全风险评估方法研究[D].北京交通大学,2018）

[24] Niesen T, Houy C, Fettke P, et al. Towards an integrative big data analysis framework for data-driven risk management in industry 4.0[C]//*2016 49th Hawaii international conference on system sciences (HICSS)*. IEEE, 2016: 5065-5074.

[25] 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.

[26] Y. Peng, K. Huang, W. Tu, et al. A Model-Data Integrated Cyber Security Risk Assessment Method for Industrial Control Systems[C]. *2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS)*, 2018, pp. 344-349.

[27] SAC/TC 310. GB/T 23694-2013: Risk management—Vocabulary[S]. Standardization Administration: Standardization Administration, 2014 (in Chinese)
（全国风险管理标准化技术委员会. GB/T 23694-2013: 风险管理——术语[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, 2013）

[28] Lockheed Martin Corporation. The Cyber Kill Chain®[OL]. [2021]. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kil

l-chain.html

[29] WANG Saie, LIU Caixia, YU Dingjiu, et al. Overview of Network Security Risk Assessment Model[J]. *Radio Communications Technology*,2020,46(04):378-384 (in Chinese)
（王赛娥,刘彩霞,俞定玖,胡鑫鑫.网络安全风险评估模型研究综述[J]. *无线电通信技术*,2020,46(04):378-384）

[30] Abdo H, Kaouk M, Flaus J M, et al. A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis [OL]. 2017. https://hal.archives-ouvertes.fr/hal-01521762.

[31] Forum of Incident Response and Security Teams. Common Vulnerability Scoring System version 3.1: Specification Document [OL]. [2021]. https://www.first.org/cvss/specification-document

[32] 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*, 2017, 16(2): 231-244.

[33] The Wikimedia Foundation. Bayes' theorem [OL]. [2021]. https://en.wikipedia.org/wiki/Bayes%27_theorem

[34] Gong Sidi. Cyber Security Risk Assessment for Industrial Control System based on Analytic Hierarchy Process and Attack Graph[D]. Nanchang Hangkong University, 2017 (in Chinese)
（龚斯谛. 基于 AHP 和攻击图的工控系统信息安全风险评估研究[D]. 南昌航空大学,2017）

[35] Joint Research Centre (JRC) EU Science Hub. eMARS. [OL]. [2021]. https://emars.jrc.ec.europa.eu/en/emars/content

[36] Software pentru comert electronic de OneLogic™. OREDA [OL]. [2021]. https://web.ordea.ro/ro/

[37] Kirwan B, Basra G, Taylor-Adams S E. CORE-DATA: a computerised human error database for human reliability support[C]. *Proceedings of the 1997 IEEE Sixth Conference on Human Factors and Power Plants*, 1997.'Global Perspectives of Human Factors in Power Generation'. IEEE, 1997: 9/7-912.

[38] Gordon Lyon (Fyodor). Nmap: the Network Mapper-Free Security Scanner [OL]. [2021]. https://nmap.org

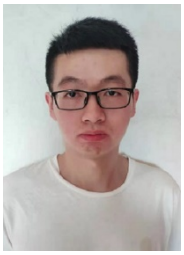
[39] Greenbone Networks GmbH. OpenVAS [OL]. [2021]. https://www.openvas.org/

[40] Fakhravar D, Khakzad N, Reniers G, et al. Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network[J]. *Process Safety and Environmental Protection*, 2017, 111: 714-725.

[41] GB/T 31509-2015: Information security technology—Guide of implementation for information security risk assessment[S]. Standardization Administration: Standardization Administration, 2017 (in Chinese)
（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）

[42] 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.

马叶桐 于 2019 年在华北电力大学信息安全专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为物联网安全、工业控制系统安全。研究兴趣包括：工控风险评估、融合安全、PLC 安全。Email：mayetong@iie.ac.cn。



丁云杰 于 2019 年在浙江大学自动化专业获得学士学位。现在中国科学院大学电子信息专业攻读硕士学位。研究领域为工业控制系统安全、物联网安全。研究兴趣包括：模糊测试、机器学习。Email：dingyunjie@iie.ac.cn。

刘圃卓 于 2018 年在吉林大学通信工程专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为物联网安全、嵌入式设备安全。研究兴趣包括：模糊测试、脆弱性分析、风险评估。Email: liupuzhuo@iie.ac.cn。

吕世超 于 2018 年在中国科学院大学信息安全专业获得工学博士学位。现任中国科学院信息工程研究所第四研究室高级工程师。研究领域为物联网安全、工业控制系统安全。研究兴趣包括：工控入侵诱捕、工控态势感知。Email: lvshichao@iie.ac.cn。

潘志文 于 2017 年在亚利桑那大学电气与计算机工程专业获得博士学位。现任中国科学院信息工程研究所副研究员。研究领域为工控安全。研究兴趣包括：时间序列异常检测、工控系统入侵检测。Email: panzhiwen@iie.ac.cn。

孙利民 于 1998 年在国防科学技术大学计算机体系结构专业获得工学博士学位。现中国科学院信息工程研究所第四研究室研究员。物联网安全、工业控制系统安全。研究兴趣包括：工控入侵诱捕、工控态势感知。Email: sunlimin@iie.ac.cn。