

文章编号: 0253-2697(2023)06-0902-15 DOI:10.7623/syxb202306002

研究动态

# 油气储运信息物理系统安全: 内涵及关键技术

张来斌<sup>1,2</sup> 汪征<sup>1,2</sup> 蔡永军<sup>3</sup> 王金江<sup>1,2</sup>

(1. 中国石油大学(北京)安全与海洋工程学院 北京 102249; 2. 应急管理部油气生产安全与应急技术重点实验室 北京 102249;  
3. 国家石油天然气管网集团公司科学技术研究总院分公司 河北廊坊 065000)

**摘要:**随着信息化和工业化的深度融合,传统油气储运逐步迈向网络化、数字化、智能化的信息物理系统。计算、通信及控制技术为油气储运行业赋能的同时带来了信息安全问题,并且发展成复杂的信息物理综合安全风险,导致叠加风险机理不清、态势感知评估困难等问题,亟需从传统以工程故障为主的物理安全分析向信息物理融合的综合风险分析转变。为此,分析了油气储运信息物理系统安全现状、内涵等相关背景,构建了围绕功能安全与信息安全一体化要素异构融合的油气储运信息物理系统安全理论技术框架,探索了信息物理系统风险形成及演化机理和风险特点,聚焦融合建模、态势感知、协同评估、异常预警、安全防护等关键技术的研究与应用,展望了信息物理系统安全的发展趋势,为推动信息物理融合安全研究提供参考。

**关键词:**信息物理系统;信息物理交互;风险形成及演化;安全态势感知;安全一体化

中图分类号:TE88

文献标识码:A

## Cyber-physical system safety for oil and gas storage and transportation: connotations and key technologies

Zhang Laibin<sup>1,2</sup> Wang Zheng<sup>1,2</sup> Cai Yongjun<sup>3</sup> Wang Jinjiang<sup>1,2</sup>

(1. College of Safety and Ocean Engineering, China University of Petroleum, Beijing 102249, China; 2. Key Laboratory of Oil and Gas Production Safety and Emergency Technology, Ministry of Emergency Management, Beijing 102249, China;  
3. PipeChina Institute of Science and Technology, Hebei Langfang 065000, China)

**Abstract:** With the deep integration of informatization and industrialization, an intelligent and digital cyber-physical system has been developing for traditional oil and gas storage and transportation. The computing, communication and control technologies empower the oil and gas storage and transportation industry, and also bring the information security issues, which will be developed into complex issues regarding comprehensive cyber-physical system safety, resulting in problems such as unclear superimposed risk mechanism and difficulties in comprehensive state evaluation. Therefore, it is urgent to change from the traditional physical safety analysis of engineering failures to the comprehensive risk analysis of cyber-physical integration. For this reason, this paper analyzes the current safety status and connotation of the cyber-physical system of oil and gas storage and transportation, establishes the cyber-physical safety theory and technology system for oil and gas storage and transportation focusing on the heterogeneous integration of functional safety and information security, explores the risk formation and evolution mechanism and risk characteristics of cyber-physical system, puts a focus on the research and application of key technologies such as fusion modeling, situation awareness, collaborative assessment, anomaly alert, and security defense, and outlook the trending study of cyber-physical system safety, thus providing a reference for pushing the research of cyber-physical system safety.

**Key words:** cyber-physical system; cyber-physical interaction; risk formation and evolution; security situation awareness; safety and security integration

引用:张来斌,汪征,蔡永军,王金江. 油气储运信息物理系统安全:内涵及关键技术[J]. 石油学报,2023,44(6):902-916,947.

Cite:ZHANG Laibin,WANG Zheng,CAI Yongjun,WANG Jinjiang. Cyber-physical system safety for oil and gas storage and transportation:connotations and key technologies[J]. Acta Petrolei Sinica,2023,44(6):902-916,947.

随着互联互通需求逐渐增加,油气储运系统已发展为典型的工业信息物理系统<sup>[1]</sup>,成为能源领域的国

家关键信息基础设施,愈加趋向大型化、复杂化、高参数化和网络化,其风险隐蔽性更强、更难辨识,被攻击

基金项目:国家自然科学基金重点项目“信息-物理视角下油气储运系统风险形成机制与控制研究”(No. 52234007)资助。

第一作者及通信作者:张来斌,男,1961年9月生,1991年获石油大学(北京)博士学位,现为中国工程院院士、中国石油大学(北京)教授,长期从事油气生产系统及装备安全科学与工程理论、方法及技术的研究工作。Email:zhanglb@cup.edu.cn

路径增多、风险链更长、波及范围广,可能危及基础设施和工业数据安全。从1982年第一个涉及关键基础设施的信息安全事件——带病的数据采集与监视控制(SCADA)软件引起西伯利亚管道爆炸<sup>[2]</sup>开始,到2021年美国最大的成品油管道公司科洛尼尔被黑客定向勒索软件攻击,导致管道控制系统停运<sup>[3]</sup>,油气储运信息安全问题不断出现,亟需研究数字化、智能化转型下的油气储运系统安全理论及关键技术。

油气储运工业控制系统是人机交互的关键,包含控制器、人机交互界面主机、SCADA服务器等典型站控设备<sup>[4-5]</sup>,控制器、通讯协议、网络节点设备以及工业控制软件存在很多未知的漏洞,易受网络攻击,尤其在油气储运行业中最典型<sup>[6]</sup>。油气储运工控防护措施以隔离控制类静态措施为主,如防火墙、网闸、数据备份等,难以适应工业系统的特点,缺少主动防御能力<sup>[7]</sup>。油气储运信息安全分析多集中于SCADA等站控、工控系统安全防护技术分析<sup>[8-9]</sup>、脆弱性分析<sup>[10]</sup>,安全风险多集中在管道、关键设备、工艺过程等物理层面,包括管道退化失效分析<sup>[11-12]</sup>、输送介质流动安全性评价<sup>[13-14]</sup>、关键设备及站场风险评价<sup>[15-16]</sup>、设备风险智能决策<sup>[17]</sup>及管网系统可靠性分析<sup>[18-19]</sup>等。

在新一代信息技术的推动下,油气储运系统不再是一个个孤岛,而是通过通信网络、信息系统、控制系统等相互耦合<sup>[20]</sup>,风险不再只与物理空间相关,还与信息空间的通信、计算等相互关联,存在多元风险及挑战,主要包括信息技术的引入、运营技术(OT)与信息技术(IT)的融合<sup>[21-22]</sup>、信息空间与物理空间高度关联3个方面。

(1) 油气储运互联互通风险:物联网、云计算、大数据等信息技术改变了油气储运孤立的系统架构,使系统运行风险多元化,安全可控性降低。油气储运从原本基于ISA-95的5层隔离架构发展为扁平化的泛在连接多元控制架构,离散化的信息系统与连续化的物理系统深度融合,系统复杂异构,交互影响日趋复杂,并且联网的工控系统风险漏洞数量多、级别高、隐蔽性强,信息物理系统互联互通,安全风险呈多元化趋势。此外,中国油气储运相关企业大力推动装备国产化战略,但压缩机组、输油泵等核心设备中关键零部件国产化率仍然较低,设备性能仍有差距<sup>[23]</sup>,核心技术受制于人,相应设备配套的管道SCADA系统等监测、控制、通信软硬件同样依赖国外厂商艾默生、西门子、Honeywell等<sup>[24]</sup>提供的运维服务,导致系统运行安全的可控性低。

(2) 油气储运IT-OT融合风险:OT与IT融合发展,系统受攻击的可能性更高。随着业务的不断扩展,

多方用户参与业务流程,油气储运行业通过新一代信息技术与业务的深度融合,运用数字化、智能化技术破解业务痛点与难点<sup>[25]</sup>。边云协同、云化SCADA等技术打破了传统工业环境相对封闭可信的状态,除了光纤通信、卫星通信、微波接力通信等传统通信技术<sup>[26]</sup>,新兴的物联网无线传输技术也被引入到智能管道中,开放的通讯控制系统使得空间跨度大、节点规模大、通信方式多的油气储运系统易受攻击,风险来源多样化。

(3) 油气储运信息物理交互风险:信息物理系统高度关联,风险影响程度及范围更大。信息系统为油气储运系统的动态感知、分析决策和精准控制提供强大支撑。但信息物理系统紧密耦合,油气能量流与通讯控制信息流交互频繁,增加节点间的风险相关性,更易形成风险链,并且信息物理系统紧密耦合,风险传播速度、影响范围大幅增加。另一方面,信息系统的失效可能经由信息物理交互作用传递到物理系统,造成故障扩大,甚至引发严重事故。

目前油气储运智能化技术不断发展,现有的油气储运安全理论方法往往单独关注信息空间和物理空间,忽略了信息系统与物理系统的交互耦合<sup>[27]</sup>,如基于事故树的扩展方法<sup>[28-29]</sup>和系统理论<sup>[30]</sup>等,或是一些基于ISO/IEC 27005、IEC 15026、IEC 62443、IEC 61511等标准制定<sup>[31]</sup>的较为初步的框架。因此,为了应对油气储运智能化转型下的综合安全理论研究的迫切需求,笔者从IT-OT融合背景下的工控安全角度分析了信息物理系统安全现状,构建了全方位、全架构、全流程的安全理论框架,阐述了信息物理安全理论的研究现状、关键技术及所面临的挑战,对推动油气储运信息物理系统的安全理论研究具有指导意义。

## 1 现状分析

油气储运类流程工业中信息与物理系统通常通过工控系统紧密联接,包含多元的系统控制、多维的系统架构及广域的系统范围(图1)。

工业信息物理系统从传统工业控制演化而来,最早可以追溯至1926年Nikola Tesla阐述了远程自动化的概念并发明了无线电遥控船。油气储运新增数据中心、云平台等信息系统优化储运过程,实现自动化和更好的性能<sup>[32]</sup>的同时,会产生网络攻击者可能利用的漏洞<sup>[33]</sup>。如图2所示,随着油气储运等工业进入智能化时代,信息物理深度融合,安全理论也需要充分利用新一代信息技术与数据资源以实现智能安全<sup>[2]</sup>。

随着信息物理系统的发展,安全理论也得到了相

应的发展,油气储运物理安全、功能安全、信息安全、功能-信息安全一体化以及信息物理安全有着许多异同点,物理安全、功能安全和信息安全针对不同的风险来源,有着互补的目标和保护对象(表1)。系统中物理安全、功能安全和信息安全相互耦合<sup>[34-36]</sup>、相互影响,信息安全在避免网络威胁下的响应活动对功能安全造成影响的条件,兼顾以保密性、完整性和可用性为目标的信息安全<sup>[37]</sup>。随着智能化发展,油气储运信息安全与物理安全风险共存、相互影响。网络威胁是攻击者的有意行为,与物理安全、功能安全不同,难以通过概率方式评估信息安全风险。信息风险通过数据链路进行传播,具有隐蔽性、突发性等特点,与传统物理风险的形成与演化机理存在较大差异,传统方法难以有

效分析信息物理环境中通信、网络安全和人为干扰等多元耦合风险扰动因素的影响。相较于传统IT,油气储运存在多元异构的攻击点和故障点,且攻击引入的风险有可能蔓延到系统的物理实体部分。油气储运控制系统对通信实时性有很高的要求,传统信息安全防护方法会导致系统功能下降<sup>[38]</sup>。因此,无论是纯粹的功能安全方法还是纯粹的信息安全方法都无法减轻系统物理基础设施的风险<sup>[39]</sup>。系统安全需要从传统以工程风险为主的物理安全分析向信息物理系统的综合分析转变,风险分析是物理安全、功能安全和信息安全的协同接口,将物理风险和网络安全作为危害分析的一部分,结合对组件之间相互作用的分析,从系统整体角度考虑信息物理综合安全问题。

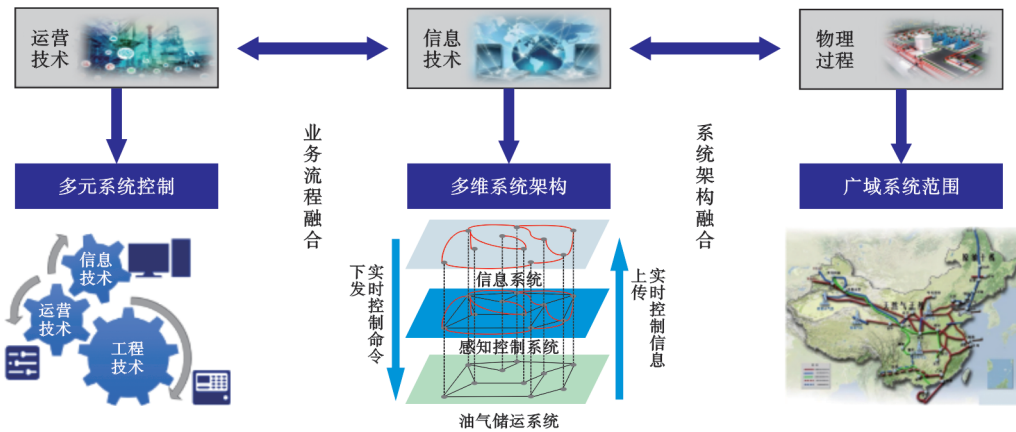


图1 传统油气储运系统到信息物理系统的转变

Fig. 1 Transformation of traditional oil and gas storage and transportation system to cyber-physical system

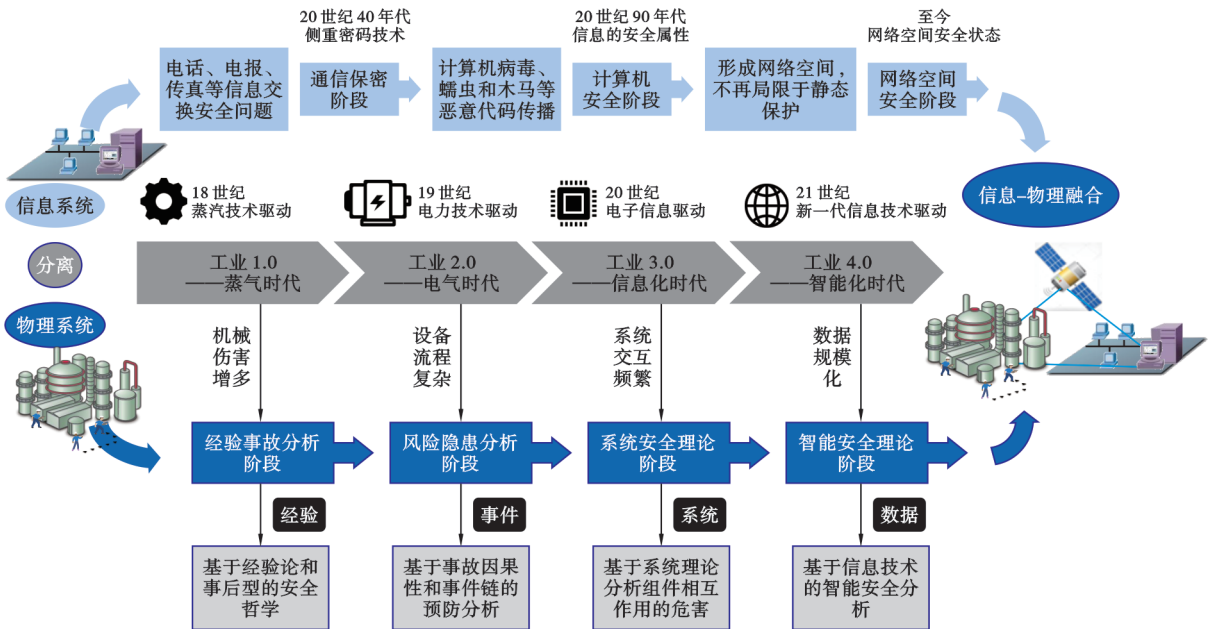


图2 安全理论的发展历程

Fig. 2 Development process of safety and security theory

表1 物理安全、功能安全、信息安全、功能信息安全一体化、信息物理系统安全概念对比

Table 1 Comparison of concepts of physical safety, functional safety, information security, integration of functional safety and information security, and cyber-physical system security

概念	研究目标	风险来源	保护对象	适用性
物理安全	减少由于电击、着火、辐射、机械危险、化学危险等因素造成的危害	物理风险:人为破坏、自然灾害和设备故障等	人员、设备、环境和财产等	“人、机、环、管”等安全要素
功能安全	安全仪表系统和其他保护层正确执行其功能,当失效或故障发生时仍能保持安全条件或进入到安全状态	功能故障:油气储运控制、感知等系统功能失效	人员、环境、设备和财产等	功能的实时性、高可用性、安全性
信息安全	保护油气工业互联网系统数据传输、处理过程,防止数据偶然或蓄意的泄露、篡改与破坏	网络威胁:拒绝服务(DoS)攻击、错误数据注入攻击(FDIA)等传统IT威胁	数据、系统、网络和用户隐私等	信息的机密性、完整性、可用性、可控性及不可否认性
功能-信息安全一体化	保护信息属性和系统功能的正常状态,以及关联风险分析处理	网络攻击、系统功能故障及其耦合影响	系统功能、数据、网络等	系统功能与信息的安全属性
信息物理系统安全	保护网络空间(Cyber)和物理空间(Physical)融合下的远离传统风险和新型综合风险	除上述风险外,涵盖整个网络空间与物理空间的风险及风险间跨域融合演化过程与影响	信息物理系统	信息物理系统中所有资产的安全属性

## 2 信息物理系统安全理论框架

### 2.1 信息物理安全内涵

信息物理安全是工业4.0智能化发展的需求<sup>[40]</sup>,是安全4.0时代<sup>[2]</sup>的一种具体体现,是为解决信息物理融合下的功能安全与信息安全相互交织、相互影响的综合分析方式。信息物理安全基于信息物理耦合视角解决系统安全问题,在工业智能化的背景下有一定的优势,能够适应复杂异构的系统环境。

油气储运信息物理安全是在“两化融合”背景下,运用大数据、人工智能、工业互联网等信息化技术,研究油气储运系统物理过程风险和网络安全威胁交互耦合机制和风险演化机理,建立系统融合建模、态势感知、异常预警等关键技术,形成装备—过程—网络一体化安全管控体系,实现全架构、全要素、全流程的融合安全。油气储运由于长期处于封闭的工业控制系统下,缺乏对现有的工控协议和软硬件在开放的网络环境下所面临的网络威胁以及后果的理解。目前的油气储运系统设计、部署、运行、维护中没有考虑综合的安全问题<sup>[41]</sup>,缺少技术、标准支撑。

由于油气储运感知与控制自动化的交互过程复杂,油气储运物理系统运行过程对信息系统具有依赖性,单个空间发生的故障或异常经过信息物理交互机制可能引起另一空间的异常,造成故障的扩大。系统的运行状态评估不仅需要考虑到物理设备的安全性,还需要考虑SCADA系统、分布式控制系统(DCS)与物理设备之间的交互以及完整性、生产管理、数据中心和自控等信息系统间的交互,以及网络攻击、数据异常等引起的系统综合态势变化。如图3所示,作为智能化趋势下的安全研究新方向,油气储运信息物理安全以

数据和模型的异构融合为主线。笔者根据其内涵将油气储运信息物理系统安全理论分为机理模型构建与多源数据分析两个层次,其相互关联、相互依托,可实现系统融合建模、风险协同评估、双侧态势感知、综合安全防护等信息物理安全技术体系。

### 2.2 信息物理安全理论技术体系

油气储运系统目前面临信息安全和物理安全高度耦合导致的风险根源辨识难、异常特征识别难、早期故障诊断预警难等问题,笔者通过对油气储运信息物理安全内涵等的分析,构建了包含机理分析、理论构建、技术实现、标准完善、全面应用五大过程的油气储运信息物理系统安全理论技术体系(图4)。风险形成及演化机理通过揭示系统运行机理、信息物理风险机理、数据关联机理,进行目标场景构建、综合风险分析、连锁关系挖掘,奠定安全理论体系基础。油气储运信息物理安全以油气储运物理系统为基础,以通信信息平台为支撑,以智能决策为手段,保障“油气流、业务流、信息流”一体化融合,全方位提升油气储运智能化管理能力和安全保障水平。通过油气储运信息物理双侧要素融合,实现物理、功能及信息安全理论一体化,从而完善现场设备、工艺过程、感知控制、网络传输、数据分析、平台应用的全架构安全保障体系。通过构建信息物理安全评价和安全防御的全过程技术实现体系,完善信息物理安全技术标准,从而具备全方位感知、综合性预判、一体化管控、自适应优化的能力<sup>[42]</sup>。

基于上述分析,笔者首先阐述了风险形成及演化机理和特征,整理了目前的信息物理安全研究焦点与难点,并阐述了其中的内在联系。分析系统的交互规则、交互路径、交互场景,继而研究风险在复杂系统中的演化过程,并研究了系统状态的感知预测。

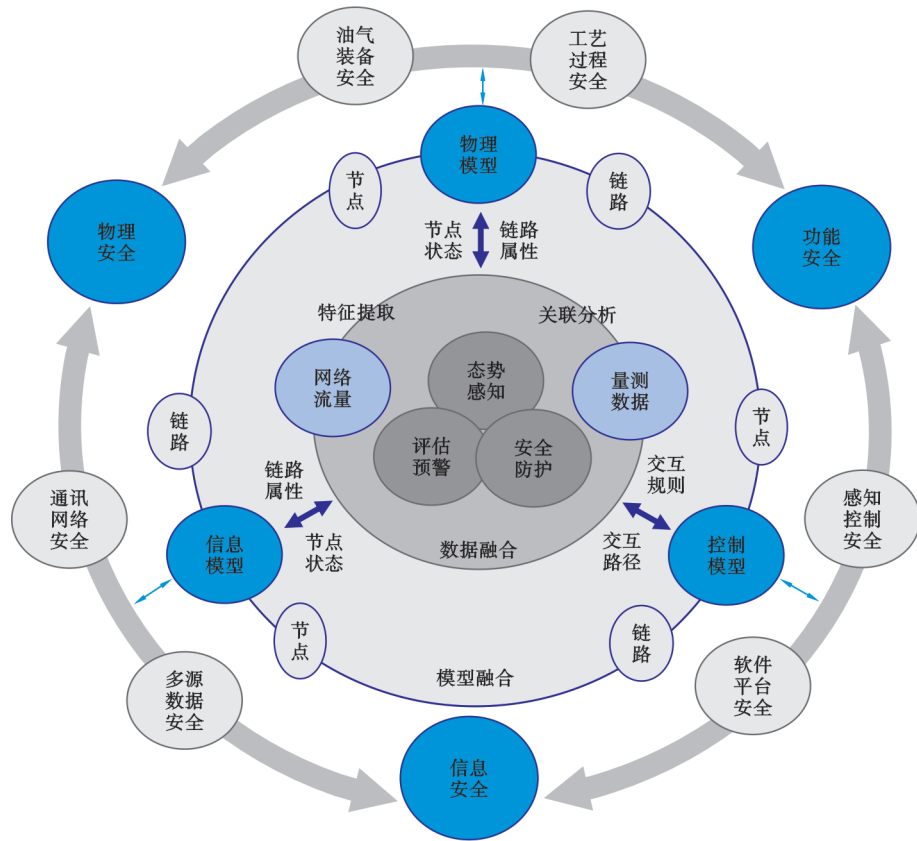


图3 信息物理安全理论内涵

Fig. 3 The connotation of cyber-physical security theory

### 2.3 风险形成及演化机理

油气储运系统同时运营两种不同类型的技术系统——信息技术和运营技术<sup>[32]</sup>。信息技术包括用于生产和通信的计算机、软件、网络设备、数据中心及云平台等,运营技术包括工业控制系统(ICS),如SCADA系统、DCS系统和可编程逻辑控制器(PLC)等。两种技术同时运用会导致油气储运网络安全防护问题,攻击者通过工业互联网访问PLC、路由器、交换机、工控软件以及通讯协议,破坏控制设备的正常连接,或是注入错误数据和命令,攻击数据传输的各个环节,涵盖执行、传感、控制决策以及应用之间的接口,对数据传输产生扰动,也可以利用工控系统软硬件漏洞进行渗透攻击,两类攻击沿着系统交互路径进行传播演化(图5)。

### 2.4 信息物理风险特征

目前油气储运信息物理系统集成度低<sup>[43]</sup>,多态的业务流程、多样的网络协议、多型的设备系统、多层的节点网络、广域的地理跨度、系统的脆弱性使得网络威胁下风险后果严重。系统交互耦合机制与原理不清,工业控制系统中漏洞攻击日趋增加,风险辨识难度大。其次,随着系统自动化程度日益提高,信息物理交互影

响日趋复杂,网络规模和量测、决策单元数量大大增加,能量流、数据流、业务流高度融合,使得原本孤立于两个空间的各类安全风险跨越原有的空间界限,传播到另一空间中,从而形成跨域风险。并且油气储运系统中信息流与能量流的频繁交互增加了各节点之间的故障相关性,风险跨域传播的可能性与传播路径亦显著增长,风险叠加发展、连锁传导,更易形成风险链。因此,油气储运信息物理系统风险后果严重、风险辨识难度大、风险跨域传播、风险耦合程度高,易导致风险根源辨识难、异常特征识别难、早期故障诊断预警难等问题。

### 2.5 信息物理系统交互影响机制

信息物理系统的结构特性与交互影响机制是系统脆弱性、可靠性分析与风险传播机理研究的基础。因此,深入研究信息系统与物理系统间的深度耦合关系,揭示信息系统和物理系统间交互影响机制是复杂信息物理系统安全研究亟需解决的首个关键科学问题。信息物理交互作用是信息物理系统的关键特征,通过管道、站场数字孪生技术将物理实体的几何形状运动行为、复杂环境等要素精准映射到信息空间并进行实时处理反馈,或是通过SCADA、DCS系统实现信息层与物理层的自动监测和控制。

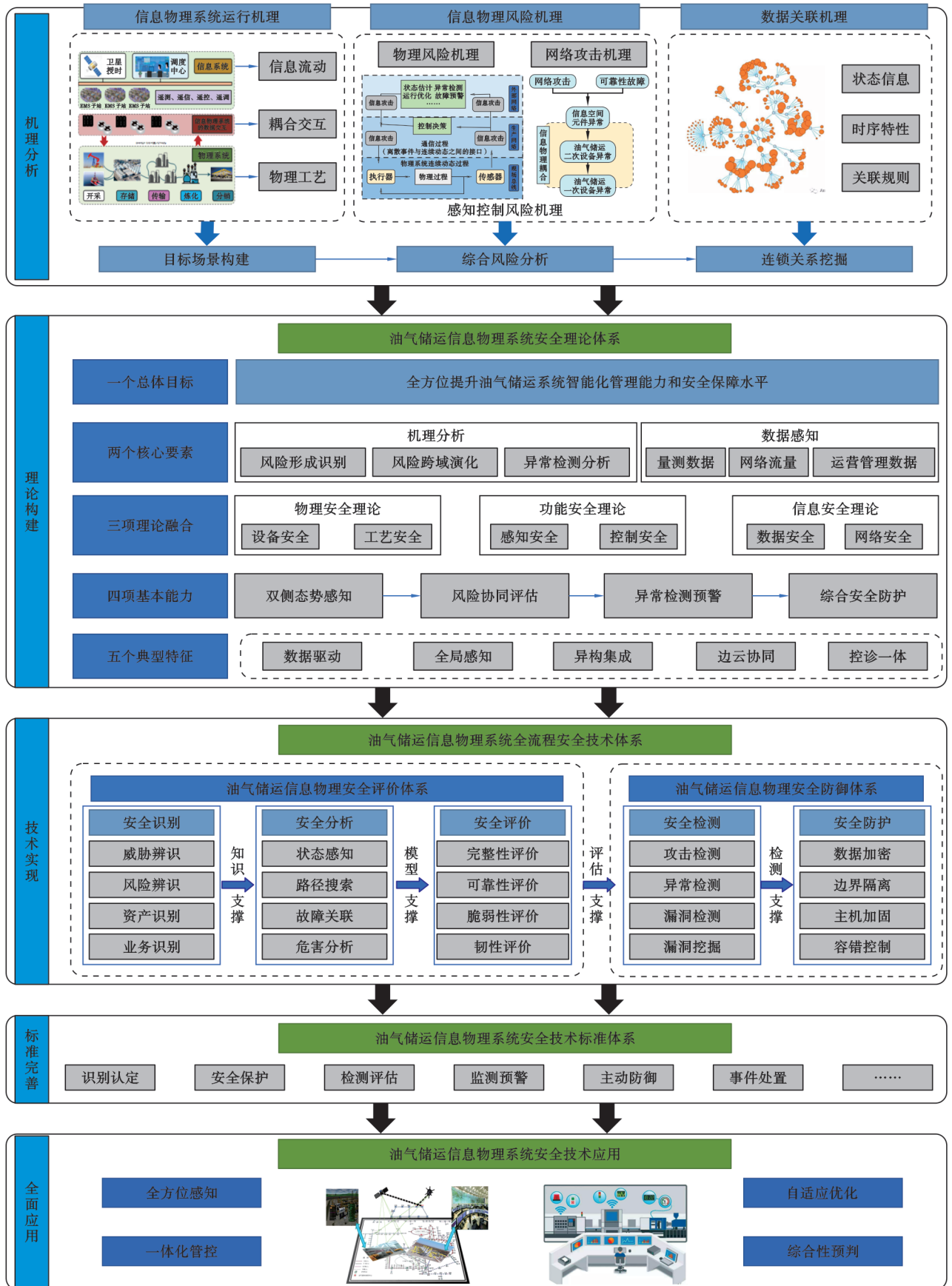


图 4 油气储运信息物理系统安全一体化理论技术体系

Fig. 4 The integrated security theory and technology system of the cyber-physical system of oil and gas storage and transportation

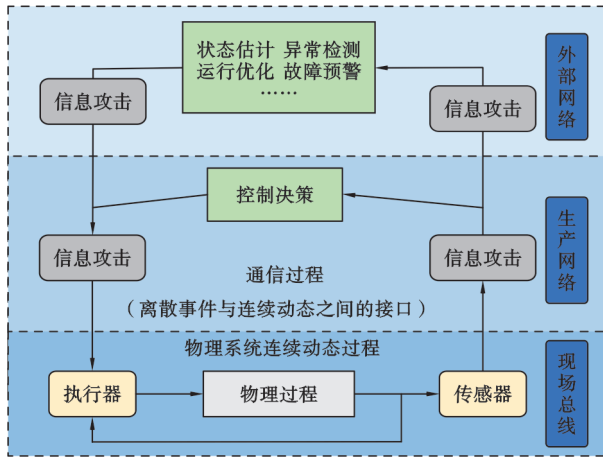


图5 风险形成及传播原理

Fig. 5 Principle of risk formation and transmission

表2 现有信息系统与物理系统间交互影响机制方法辨析

Table 2 Analysis of interaction mechanism and methods between the existing information system and physical system

出发点	一般流程	典型方法	作用	局限性
图形	对信息层、物理层与通信层进行建模;通过关联特性矩阵等方法将物理实体层、信息物理耦合层、信息系统层联通起来并求解	图论、复杂网络理论等	重点关注系统的拓扑结构特性,能够有效分析系统结构脆弱性、可靠性	忽略网络物理属性
混合系统	建立混合系统的数学模型,混合系统包括时间驱动部分和事件驱动部分	混合逻辑动态模型(MLD) + 有限状态机(FSM)、Petri网等	重点关注信息物理交互作用,并且可用于系统的优化控制、系统韧性分析	关注自动化控制过程,缺乏系统高度的认识
高级建模语言	将CPS分解为若干用不同模型表示的部分,再考虑不同模型之间的映射	体系结构分析与设计语言(AADL)等	简单的语法、强大的功能和可扩展性	信息域与物理域模型的实施映射与兼容困难

了网络脆弱性;文献[47]建立了基于CPS的智能制造资源自主协作网络,利用加权复杂网络理论构建小世界模型并分析网络拓扑;文献[48]建立了上海供水系统复杂网络,并通过社团检测算法和频谱分析孤立群体;在电力领域的大量研究<sup>[49-52]</sup>中构建了小世界、无标度及随机网络等静态网络模型,随着研究的深入,信息物理耦合关系得到了重视,文献[53-55]构建了节点一对一、一对多以及部分节点相连接的多层次耦合复杂网络电力CPS模型。

由于信息物理系统伴随工控自动化而产生,控制领域的研究也逐渐向信息物理系统发展。文献[56]从信息系统对物理系统的作用角度将离散信息量作为物理设备模型的一种输入变量进行建模;文献[57]考虑CPS内部的交互、分布式管理和控制等特征,利用系统理论的方法进行安全分析;文献[58]通过构建CPS中各类事件之间驱动关系,使信息流与能量流的交互作用得以明确阐述;除此之外,混合系统理论的研究较为集中,文献[59]提出了基于Petri网的CPS时空模型,建立了车对车的通信模型;文献[60]将CPS概念和感知控制论相结合,构建化工过程安全信息物理融合系统模型;文献[61-63]从控制角度出发,构造了FSM五元组模型,将其转化为MLD模型,建立主动

油气储运信息物理交互研究匮乏,其他领域信息物理系统交互分析目前多集中于信息空间与物理系统的交互拓扑、离散信息状态与连续物理过程的相互作用等,研究方法分为图形、混合系统、高级建模语言3类(表2)。

图形建模方法关注系统拓扑结构,采用图形的方法对系统进行融合建模,多用于系统拓扑结构的脆弱性、可靠性研究。文献[44]基于图论将成品油管道管网抽象为节点与边以用于故障诊断。随着系统结构逐步大型化、复杂化,复杂网络理论应用越来越广泛,而油气储运行业领域仍停留在将复杂网络应用于物理层风险的演化分析<sup>[45]</sup>。在其他行业中,文献[46]建立了酸浸冶炼生产物理信息系统复杂网络模型,初步分析

配电网模型,并且构建了一种基于MLD和Ptolemy II的电力信息物理系统模型。

信息物理系统的发展离不开现代计算机技术,原本针对嵌入式系统的高级建模语言AADL由于其标准化、语义强大、扩展性强得到了大量扩展,文献[64-70]从不同的出发点扩展了AADL语言对CPS融合的建模。

综上所述,目前关于信息物理系统交互机制多是自下而上的视角,关注点还在于底层的工业控制器与现场设备的交互,难以有效解释油气储运信息物理系统运行机制和系统运行状态的演化过程。电力系统大量研究关注信息物理系统融合建模,而与电力网络拥有类似特点的油气管网融合建模却鲜有研究。此外,目前融合建模方法普遍存在无法兼顾网络拓扑结构和物理属性的局限性,难以分析油气储运信息物理系统的网络拓扑、设备设施及工艺过程可靠性。由于信息物理系统同时存在连续的物理层和离散的信息层,油气储运等流程工业实时性要求高,阐述信息层与物理层的交互机制与实现融合建模并保持系统的实时性是当前研究的难点。

## 2.6 信息物理系统跨域风险演化机理

油气储运系统是物理系统与信息系统的深度融合,系统内部控制系统交互需求大,交互路径复杂,采

取大量不同的网络协议,包含有线、无线各类传输方式。单个空间发生的故障或异常经过以上交互过程可能引起另一空间的异常,造成故障的扩大。因此,研究信息物理系统风险成因与演化过程,阐明风险跨空间传播机制,揭示信息物理跨域风险演化机理,是油气储运系统安全理论研究的重点与核心。信息物理系统风险研究的关键在于明确系统的风险点、风险在不同的

空间中传递的规则、双侧风险之间的关联关系以及危害后果与场景。

目前油气储运安全风险研究大多关注 CPS 物理空间的风险及其故障传播机制与方式,并且其他领域对信息物理交互影响下跨域风险传播与演化机理研究也较为初步,主要集中于信息物理双侧风险融合辨析与网络攻击及演化模型构建(表 3)。

表 3 现有信息系统与物理系统风险分析方法辨析

Table 3 Analysis of existing risk analysis methods between information system and physical system

阶段	主要方法	特征描述
风险辨析	目标结构符号(GSN) <sup>[55]</sup> 、信息和能量的非受控流动方法(UFoI-E)、STPA 扩展方法、HAZOP 扩展方法、FMEA 扩展方法等	宏观的风险识别、分析及措施框架,集成了物理风险与网络威胁
风险演化	故障树扩展、电力系统方法、统一建模语言 UML(CHASSIS、UMLsec/safe、SysMLsec 等)、Petri 网、贝叶斯信念网络 BBN、马尔可夫过程、AADL 等	系统功能和系统风险的演化形式化或半形式化表达

### 2.6.1 信息物理双侧风险辨析方面

在信息物理双侧风险辨析方面,国内外研究主要是早期的、定性的方法,集中于构建统一的框架或采用集成的方法进行风险枚举,适用于大多数行业,但基于 HAZOP 的信息安全化拓展方法<sup>[71]</sup>和基于失效模式与影响分析(FMEA)的信息层拓展方法<sup>[72]</sup>属于早期的、定性的风险辨识方法;结合网络的保护层分析(LOPA)<sup>[73]</sup>、信息和能量的非受控流动方法(UFoI-E)<sup>[74]</sup>、系统理论过程分析(STPA)扩展方法<sup>[75]</sup>等各类形式化或半形式化方法,主要用于识别 CPS 中的危害情景;此外,基于模型的 CPS 安全风险评估方法<sup>[76]</sup>利用混合自动机推导出物理系统的数学模型来列举系统的潜在危险状态。

### 2.6.2 风险演化机理方面

与以往的研究不同,风险演化存在跨越离散信息域和连续物理域的过程,目前多集中于单一行业的特性分析,缺少共性分析,或是基于传统安全分析方法进行改进用于分析信息侧网络攻击。文献[77]提出了考虑物理层电网潮流分析与信息层延时的信息物理系统电力系统连锁故障模型;文献[78]考虑电网运行过程、信息传递和处理过程三者间的交互机制,分析了网络攻击下的信息风险传播原理;文献[79]建立了主动配电网信息攻击下的风险传递模型,揭示故障在配电网信息物理系统中的演化机理。也有大量研究基于网络攻击的角度建立风险的传递模型,如文献[80]描述了受网络攻击的 CPS 动态数学模型,将 CPS 遭受网络攻击时的安全属性作为映射函数,提出了一种安全评估模型;此外,还有故障树扩展方法<sup>[81]</sup>、Petri 网<sup>[82]</sup>、统一建模语言<sup>[83-85]</sup>、信赖贝叶斯网络<sup>[86]</sup>等基于故障树分析的风险演化模型。

综上所述,上述工作多局限在组件、功能或部分应

用层等子系统的分析,风险辨识还处于早期的、定性的阶段,油气储运在信息物理融合条件下,风险后果严重、风险辨识难度大、风险跨域传播、风险耦合程度高,安全风险要素与风险演变机制仍不明确,信息物理交互影响诱发的叠加风险阐述不清,缺乏对信息物理系统跨域风险传递与演化描述的理论框架。

## 2.7 信息物理系统多源异构数据融合感知

态势感知<sup>[87]</sup>主要分为态势觉察、态势理解以及态势投射 3 部分。目前油气储运系统中有着各类信息系统,主要包含应用集成系统、生产管理系统、完整性管理系统、SCADA 系统、管道环境监测系统等。如何在数据层面集成各大系统数据,合理利用大数据技术实现运行状态监控数据高效挖掘、融合以及系统安全状态全面评估是信息物理深度融合下态势感知评估的关键。因此,研究复杂异构数据融合分析方法,提出信息物理深度融合下系统态势感知评估策略是油气储运系统安全理论研究的关键。目前关于态势感知的研究多集中于工控系统和电网两个领域,而在油气储运领域将信息系统和物理系统融合的协同态势感知研究成果较少。针对油气储运系统特点,态势觉察的关键在于信息物理双侧的信息提取,而在态势感知要素及数据分析方面主要是一些针对感知要素的初步分析。文献[88]分析了 CPS 态势感知要素,其既包括实时在线数据,也包括设备参数信息和网络拓扑模型等离线信息;文献[89]明确了能源管道安全态势感知能力组成和数据采集范围。针对信息物理系统的攻击检测是要素感知的重要研究点,文献[90]建立了 CPS 的 SCADA 信息流状态转移图,提出了基于关系流程图的入侵检测思想,以检测错误数据注入攻击;文献[91]定义了对网络控制系统的欺骗和拒绝服务攻击。

态势理解和态势投射是对态势感知要素的分析与



应用,需要重点研究态势感知分析/状态估计,关键在于信息物理双侧的数据融合。目前研究大都集中于状态数据的分析,文献[92]采用改进的C-支持向量分类算法对多源数据进行规则提取,最终融合获取态势感知结果;文献[93]研究基于改进鲁棒估计的电力CPS状态辨识方法,建立多能源数据驱动的综合态势感知模型;文献[94]针对海上油气压缩过程控制系统安全设计了一种能够识别影响物理系统完整性安全事件的风险定性评估方法。此外,较多研究根据网络攻击制定了解决方案,文献[95]分析了输气管道SCADA网络安全策略,提出安全威胁检测方案;文献[96]为增强CPS网络安全以及网络攻击容忍度,采用模块化的方式开发安全评估/增强平台,分析网络漏洞和监控平台运行。

综上所述,目前国内外研究多是对单个系统的态势感知或者异常检测,其在其他领域已有相关框架,但是从CPS整体视角建模分析的研究仍停留在理论层面,有效成果较少。原因在于,一方面忽略了系统的其他安全状态特性,另一方面缺乏考虑系统交互影响,对CPS全局态势感知和异常检测的研究尚处于起步阶段。

### 3 关键技术

基于以上分析,现阶段油气储运信息物理系统安全技术研究未能充分利用新一代信息技术的优势,信息物理交互影响下的安全技术需要进一步提升。笔者提出了信息物理系统五大安全关键技术,阐述了信息物理系统交互过程,完成了信息物理双侧的数据治理与融合,充分发挥了双侧系统感知技术数据感知能力,实现了风险主动辨识、安全主动防御,使油气储运信息与物理的安全技术从分离状态走向信息物理系统的技术融合,系列技术方法的共同支撑,保证了理论体系的可实践性(图6)。

#### 3.1 油气储运信息物理系统融合建模技术

油气储运信息物理系统存在多态的业务流程、多样的网络协议、多型的设备系统、多层的节点网络等特点,难以精准分析系统状态。

系统融合建模是指信息物理双侧的机理、模型的融合,通过分析双侧异构的连续-离散系统,分析信息物理交互拓扑以构建信息空间与油气储运物理系统交互场景,进而建立离散信息空间状态变量与连续油气工艺过程变量的多维耦合数学模型,发掘系统交互路径,依据图论、复杂网络理论等建立信息物理关键交互路径搜索方法,再对所建立的模型中的节点、链路等进行关联分析、特征提取与融合等操作,优化融合模型。

但目前信息物理系统架构不明确,交互分析仅从工控领域CPS的交互分析手段出发,难以准确刻画信息离散状态与连续过程的动态交互过程。

#### 3.2 油气储运信息物理系统综合态势感知技术

油气储运系统数据多源异构、规模大、融合分析难,随着管网规模持续扩大,监控数据种类和规模不断增加,所采集的数据呈爆发式增长;同时各监控系统相互独立,数据结构、运行机制存在差异,导致数据冗余。

态势感知是针对信息物理双侧数据分析的融合,是油气储运系统安全稳定运行的基础。随着信息物理系统的全面融合,态势感知难度持续升级。建立系统动态感知模型需要获取信息侧网络流量和物理侧管网量测数据以量化系统状态,结合系统交互和风险演化引起的系统状态动态变化,从而实现油气储运系统态势感知要素提取与分析,应用聚类分析、关联规则挖掘等方法剔除异常数据,提出多源异构数据驱动的态势感知方法。如何在有限的计算、通讯资源约束下,协调系统差异,从大数据中挖掘和提取有效信息,对多源异构数据进行融合分析,是油气储运系统信息物理安全的关键。

#### 3.3 油气储运信息物理系统风险协同评估技术

信息物理深度融合下油气储运系统的运行状态评估不仅需要考虑物理设备的安全性,还需要考虑信息系统网络攻击、数据异常等引起的系统综合态势变化。信息物理系统多层次影响因素交互耦合,协同评估难,油气储运信息物理系统运行过程易受到来自物理系统及信息系统的多元因素影响。目前的研究一方面忽略了系统的其他安全状态特性,另一方面缺乏考虑系统交互影响,具体的有效成果较少。因此,对其进行评估时,必须考虑物理系统和信息系统之间的耦合关系以及跨域风险传播与故障演化影响因素,构建多层级风险因素分析框架以辨识多元风险,形成风险、漏洞与威胁库,采用复杂网络理论分析级联风险演化过程,建立跨域风险演化模型,依据油气控制过程的数据求解系统状态,对信息物理跨域风险演化进行量化评估。

#### 3.4 油气储运信息物理系统异常检测预警技术

油气储运关键设备种类繁多、数量庞大,设备自身运行异常也会导致数据异常。信息物理双侧空间异常检测存在难度,异常特征辨识难。油气储运系统运行过程中也存在着多种不确定因素,易受多样化网络攻击,从而在数据层面上显示异常,设备故障会直接影响信息系统的态势感知,而网络攻击也会导致物理设备的执行故障,这些因素间存在着隐蔽性和复杂的关联性,导致系统报警频繁。



图 6 信息物理安全关键技术

Fig. 6 Key technologies of cyber-physical system security

如何利用数据驱动方法构建异常检测模型以及基于双侧特征的异常检测方法,对各类网络协议进行深度解读,对现有的攻击手段实时响应,对异常流量进行解读,从而实现跨空间的连锁故障诊断。分析具有时

序性的双侧异常数据,依靠决策分类算法训练跨空间连锁风险历史数据,建立跨空间连锁风险早期预警机制,是油气储运信息物理系统异常检测预警技术的关键难题。

### 3.5 油气储运信息物理系统综合安全防护技术

目前油气储运安全防护存在的防御方案基本都采用静态的被动防御技术,风险分析不全面,安全防护研究大都也只考虑信息威胁或物理风险,忽视信息物理一体化安全,亟需研究综合安全防护。

综合安全防护是以“一个中心、三重边界、四大技术”为主线:一个中心是安全管理中心,其统筹管理油气储运信息系统和物理系统全局状态、网络态势可视化;油气储运控制网络中三重边界是生产网络边界、外联网络边界、主机等终端边界;各类边界的防护各有差异,因此将安全防护分为主机加固、边界隔离、审计监控、主动防御四大技术。

## 4 发展趋势

随着信息技术的发展与应用,油气储运信息空间与物理空间不断融合,促使传统安全理论发生重要变革,朝着信息物理融合的安全理论研究发展。针对信息物理系统安全问题,国内外学者做了大量研究,但油气储运领域信息物理安全研究较少,并且未结合油气储运大型化、复杂化、广域化等特点从系统的高度对信息物理安全的研究需求、研究方法、研究目标进行体系化的描述。具体而言:①信息物理系统交互机制尚不明确,融合模型不够贴合实际,无法满足对信息物理系统风险的分析;②风险演化的研究较为初步,大都基于网络攻击建模,未考虑信息物理融合下风险的依赖与对抗关系;③态势感知中要素的提取和分析仍停留在理论框架的构建、数据的提取与融合,其应用仍不成熟。这一系列信息物理系统安全理论研究问题的本质是安全理论信息物理融合程度不适应、不匹配信息物理系统高度耦合的现状,因此信息物理系统安全理论的发展需要描述尽可能贴近现实的油气储运信息物理系统以及系统交互等的动态过程,需要功能与信息安全进一步融合,需要双侧系统感知进一步融合以发挥数据作用,实现主动防御。

### 4.1 交互耦合紧密化

目前油气储运信息物理系统智能化、信息化程度还处于一个较低的水平,且交互松散、机制不明确。随着智能化程度不断提高,油气储运从原本基于 ISA-95 的 5 层隔离架构发展为扁平化的泛在连接多元控制架构,离散化的信息系统与连续化的物理系统深度融合,OT 与 IT 的融合发展,边云协同、云化 SCADA 等技术通过有限传输、新兴的物联网无线传输连接物理设备,使得交互变得频繁,现场射频识别、视频监控、智能传感器系统逐渐增多,连接需求和类型陡增。

由于油气储运信息物理系统是包含动态多变、复

杂异构过程的系统,对其进行一体化的建模与交互分析较难实现,油气行业传统分析方法难以奏效。因此,仿真分析是理论发展的基础,国内外普遍通过开发一个有效的仿真实验平台来分析 CPS 的交互机制,以分析系统的脆弱性,并验证相关安全理论技术。通过仿真实验平台来模拟或者还原发生在油气生产真实系统上的物理事件、控制交互过程以及网络安全事件真相,还能够展现攻击渗透对真实油气环境产生的影响和危害,研究如何通过安全防护手段来抵御面临的安全威胁以及验证防护手段的有效性等,但目前仿真平台存在亟需解决的一体化仿真统一建模难、联合仿真协同同步难等问题。

### 4.2 功能-信息安全一体化

智慧管网建设是工业 4.0、信息物理系统等发展趋势下“两化”深度融合的主攻方向和突破口,在新态势下,同步推进功能-信息安全一体化保障体系具有重大战略意义。当前,油气储运系统中智能生产、感知、控制设备广泛分布于系统之中,无人化程度高、灵活性强,出现网络攻击及涉及设备增多,但是通过智能化提升设备可靠性还在发展过程中,综合信息空间与物理空间的安全问题不断增长与恶化,需要不断耦合与演化,因此一体化安全理论研究需求日益迫切。

开展面向安全一体化设计及实施技术和标准的研究,涵盖传统油气储运行业风险与 IT 行业网络威胁,并结合油气储运环境特点下的关联风险、融合风险,探索与解决油气功能安全与信息安全融合与协调问题,建立全生命周期、全架构保障、全流程管理的安全方案,改变传统油气储运研究中功能安全、信息安全独立的现状,避免由于只关注信息安全使得生产力下降,无法保证实时性,或只关注功能安全,而使关键信息泄露、系统遭受网络攻击全面失效。

### 4.3 安全防护主动化

目前油气储运工控系统安全防护的防御方案基本都采用静态的被动防御技术,以隔离类设备为主,根据防护需求的不同,在油气储运系统中部署的位置不同,通常用于各层级、各区域之间的基于 TCP/IP 工业控制协议防护。和传统 IT 信息安全问题不同,油气储运信息物理系统实时性、可用性要求高,阻断防护技术引入了潜在的风险点,需要审计监控、隔离防护、检测预测综合安全防护。因此,研究油气储运工业物联网基础架构的风险来源,辨识系统中的风险因素并且构建不同层级的风险因素体系框架,建立完整的系统感知过程,充分利用信息物理双侧数据,通过深入理解底层数据来精准保障系统安全,使得信息物理双侧态势感知从理论框架走向技术应用,进行攻击预测、攻击过

程建模、安全协同评估等,构建新一代工控系统 OT-IT 融合的主动安全防御体系。

## 5 结 论

(1) 为深入研究与发展信息物理安全理论和技术,分析了信息物理系统及油气储运安全理论发展现状,以信息物理交互耦合、风险演化、态势感知为导向,探索发现了传统安全理论和方法在工业 4.0 背景下的局限性,指出油气储运信息物理安全理论研究匮乏现状与管网智能化发展的需求不适应。

(2) 从系统级视角出发,定义了油气储运信息物理系统的安全内涵,围绕功能安全与信息安全的融合分析,以数据、模型、机理、风险等要素的异构融合为主线,构建了涵盖机理分析、理论构建、技术实现、标准完善和全面应用等方面的油气储运信息物理系统安全理论与技术体系。

(3) 指出了区别于传统油气储运的风险形成及演化机理和风险特征,对信息物理系统安全理论研究进行了综述,并总结了信息物理安全理论研究的现状与挑战。

(4) 从多个层面的信息物理要素融合探讨了油气储运信息物理安全关键技术,为实现信息物理融合安全理论技术实现与应用提供参考。

(5) 根据油气储运实际需求与问题,提出了未来系统交互紧密化、安全一体化、防御主动化等理论技术及应用的发展趋势。

### 参 考 文 献

- [1] WANG Dong, WANG Zidong, SHEN Bo, et al. Recent advances on filtering and control for cyber-physical systems under security and resource constraints[J]. *Journal of the Franklin Institute*, 2016, 353(11): 2451-2466.
- [2] SÁNCHEZ H S, ROTONDO D, ESCOBET T, et al. Bibliographical review on cyber attacks from a control oriented perspective [J]. *Annual Reviews in Control*, 2019, 48: 103-128.
- [3] TSVETANOV T, SLARIA S. The effect of the Colonial Pipeline shutdown on gasoline prices[J]. *Economics Letters*, 2021, 209: 110122.
- [4] 陈浩, 沈博臣, 钱泓超. 油气管道运输中的工艺设备与自动化控制[J]. *制造业自动化*, 2021, 43(08): 69-73.  
CHEN Hao, SHEN Bochen, QIAN Hongchao. Process equipment and automatic control in oil and gas pipeline transportation [J]. *Manufacturing Automation*, 2021, 43(08): 69-73.
- [5] 张小虎, 蒋丽琼. 长输天然气管道站控系统工控安全方案设计与研究[J]. *信息安全研究*, 2019, 5(8): 740-745.  
ZHANG Xiaohu, JIANG Liqiong. Research on security protection for station control system of long-distance natural gas transmission pipeline[J]. *Journal of Information Security Research*, 2019, 5(8): 740-745.
- [6] 王保庆. 油气管道工控系统网络安全问题探讨[J]. *中国石油和化工标准与质量*, 2020, 40(8): 82-84.  
WANG Baoqing. Discussion on network security issues of oil and gas pipeline industrial control system[J]. *China Petroleum and Chemical Standard and Quality*, 2020, 40(8): 82-84.
- [7] 程小曼, 黄茜, 赵萍萍, 等. 油气 SCADA 系统安全主动防御体系构建及应用[J]. *网络安全和信息化*, 2022(1): 139-142.  
CHENG Xiaoman, HUANG Qian, ZHAO Pingping, et al. Construction and application of active defense system for oil and gas SCADA system security[J]. *Cybersecurity & Informatization*, 2022(1): 139-142.
- [8] 郭建军. 长输天然气管道 SCADA 系统信息安全现状分析及优化措施[J]. *电子世界*, 2020(20): 74-75.  
GUO Jianjun. Analysis of information security status and optimization measures of SCADA system for long-distance natural gas pipelines[J]. *Electronics World*, 2020(20): 74-75.
- [9] 刘锐, 薛金良, 张志群, 等. 油气管道 SCADA 系统工控安全策略研究与实现[J]. *自动化应用*, 2021(9): 168-172.  
LIU Rui, XUE Jinliang, ZHANG Zhiqun, et al. Research and implementation of industrial control security strategy for oil and gas pipeline SCADA system[J]. *Automation Application*, 2021(9): 168-172.
- [10] 刘锐, 薛金良, 包贤晨, 等. 油气管道 SCADA 系统工控安全分析[J]. *信息技术与网络安全*, 2021, 40(11): 1-7.  
LIU Rui, XUE Jinliang, BAO Xianchen, et al. Industrial control security analysis of SCADA system for oil and gas pipeline[J]. *Information Technology and Network Security*, 2021, 40(11): 1-7.
- [11] 张宏, 吴锴, 冯庆善, 等. 高钢级管道环焊缝断裂韧性与裂纹拘束关系[J]. *石油学报*, 2023, 44(2): 385-393.  
ZHANG Hong, WU Kai, FENG Qingshan, et al. Relationship between fracture toughness and crack tip constraint of high-strength pipe girth welds[J]. *Acta Petrolei Sinica*, 2023, 44(2): 385-393.
- [12] 杨永, 罗艳龙, 孙明, 等. 油气管道交流杂散电流腐蚀研究进展[J]. *石油学报*, 2021, 42(9): 1247-1254.  
YANG Yong, LUO Yanlong, SUN Ming, et al. Research advances in stray alternating current corrosion of oil and gas pipelines[J]. *Acta Petrolei Sinica*, 2021, 42(9): 1247-1254.
- [13] 马大中, 胡旭光, 孙秋野. 基于大维数据驱动的油气管网泄漏监控模糊决策方法[J]. *自动化学报*, 2017, 43(8): 1370-1382.  
MA Dazhong, HU Xuguang, SUN Qiuye. A large dimensional data-driven fuzzy detection method for oil-gas pipeline network leakage[J]. *Acta Automatica Sinica*, 2017, 43(8): 1370-1382.
- [14] 何利民, 梁隆杰, 黄天山. 石油储运设施衍生的多场景灾害评价技术[J]. *油气储运*, 2021, 40(9): 1063-1071.  
HE Limin, LIANG Longjie, HUANG Tianshan. Assessment technology of multi-scenario disasters derived from oil storage and transportation facilities[J]. *Oil & Gas Storage and Transportation*, 2021, 40(9): 1063-1071.
- [15] 王金江, 张来斌, 蔡永军. 油气站场风险评估[M]. 北京: 石油工业出版社, 2020.  
WANG Jinjiang, ZHANG Laibin, CAI Yongjun. Risk assessment of oil and gas stations[M]. Beijing: Petroleum Industry Press, 2020.
- [16] 王新, 刘建平, 张强, 等. 油气管道定量风险评估技术发展现状及对策[J]. *油气储运*, 2020, 39(11): 1238-1243.

- WANG Xin, LIU Jianping, ZHANG Qiang, et al. Development status and countermeasures of quantitative risk assessment technology for oil & gas pipeline[J]. *Oil & Gas Storage and Transportation*, 2020, 39(11): 1238-1243.
- [17] 王金江, 王舒辉, 张来斌, 等. 基于数字孪生的压气站场设备风险智能决策系统[J]. *天然气工业*, 2021, 41(7): 115-123.  
WANG Jinjiang, WANG Shuhui, ZHANG Laibin, et al. Digital twin based intelligent risk decision-making system of compressor station equipment[J]. *Natural Gas Industry*, 2021, 41(7): 115-123.
- [18] 黄维和. 大型天然气管网系统可靠性[J]. *石油学报*, 2013, 34(2): 401-404.  
HUANG Weihe. Reliability of large-scale natural gas pipeline network[J]. *Acta Petrolei Sinica*, 2013, 34(2): 401-404.
- [19] 肖峻, 宋晨辉, 鲍震宇, 等. 天然气管网系统的稳态安全域模型[J]. *石油学报*, 2021, 42(8): 1103-1112.  
XIAO Jun, SONG Chenhui, BAO Zhenyu, et al. Steady-state security region model of the natural gas transmission system[J]. *Acta Petrolei Sinica*, 2021, 42(8): 1103-1112.
- [20] 张劲军, 苏怀, 高鹏. 天然气管网韧性保供问题及其研究展望[J]. *石油学报*, 2020, 41(12): 1665-1678.  
ZHANG Jinjun, SU Huai, GAO Peng. Resilience-based supply assurance of natural gas pipeline networks and its research prospects[J]. *Acta Petrolei Sinica*, 2020, 41(12): 1665-1678.
- [21] AGARWAL N, BREM A. Strategic business transformation through technology convergence: implications from General Electric's industrial internet initiative[J]. *International Journal of Technology Management*, 2015, 67(2/4): 196-214.
- [22] LARA P, SÁNCHEZ M, VILLALOBOS J. Enterprise modeling and Operational Technologies (OT) application in the oil and gas industry[J]. *Journal of Industrial Information Integration*, 2020, 19: 100160.
- [23] 杨喜良, 张栋, 蔡永军. 油气管道关键设备国产化探索与实践[J]. *油气储运*, 2021, 40(1): 7-14.  
YANG Xiliang, ZHANG Dong, CAI Yongjun. Exploration and practice of key equipment localization in oil and gas pipelines[J]. *Oil & Gas Storage and Transportation*, 2021, 40(1): 7-14.
- [24] 李柏松, 徐波, 王巨洪, 等. 中俄东线北段关键设备与核心控制系统国产化[J]. *油气储运*, 2020, 39(7): 749-755.  
LI Baisong, XU Bo, WANG Juhong, et al. Localization of key equipment and core control system in north section of China-Russia Eastern Gas Pipeline[J]. *Oil & Gas Storage and Transportation*, 2020, 39(7): 749-755.
- [25] 杨剑锋, 杜金虎, 杨勇, 等. 油气行业数字化转型研究与实践[J]. *石油学报*, 2021, 42(2): 248-258.  
YANG Jianfeng, DU Jinhu, YANG Yong, et al. Research and practice on digital transformation of the oil and gas industry[J]. *Acta Petrolei Sinica*, 2021, 42(2): 248-258.
- [26] 刘桂志. 智能管道物联网网络层构建技术[J]. *油气储运*, 2021, 40(5): 515-520.  
LIU Guizhi. Construction technology of Internet of Things network layer for intelligent pipelines[J]. *Oil & Gas Storage and Transportation*, 2021, 40(5): 515-520.
- [27] 薛禹胜, 李满礼, 罗剑波, 等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. *电力系统自动化*, 2018, 42(2): 11-19.  
XUE Yusheng, LI Manli, LUO Jianbo, et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. *Automation of Electric Power Systems*, 2018, 42(2): 11-19.
- [28] OVEISI S, RAVANMEHR R. SFTA-based approach for safety/reliability analysis of operational use-cases in cyber-physical systems[J]. *Journal of Computing and Information Science in Engineering*, 2017, 17(3): 031018.
- [29] ALI N, HUSSAIN M, HONG J E. Analyzing safety of collaborative cyber-physical systems considering variability[J]. *IEEE Access*, 2020, 8: 162701-162713.
- [30] SPAN M T, MAILLOUX L O, GRIMAILA M R, et al. A systems security approach for requirements analysis of complex cyber-physical systems[C]// *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. Glasgow: IEEE, 2018: 1-8.
- [31] JI Zuzhen, YANG Shuanghua, CAO Yi, et al. Harmonizing safety and security risk analysis and prevention in cyber-physical systems[J]. *Process Safety and Environmental Protection*, 2021, 148: 1279-1291.
- [32] 王现中. 油气储运智能化研究进展[J]. *当代化工研究*, 2020(18): 7-8.  
WANG Xianzhong. Research progress of intelligent oil and gas storage and transportation[J]. *Modern Chemical Research*, 2020(18): 7-8.
- [33] Congressional Research Service. Pipeline cybersecurity: Federal Programs[R]. Washington, D. C.: Library of Congress, 2019.
- [34] PIÈTRE-CAMBACÉDÈS L, CHAUDET C. The SEMA referential framework: avoiding ambiguities in the terms "security" and "safety"[J]. *International Journal of Critical Infrastructure Protection*, 2010, 3(2): 55-66.
- [35] XIONG Wenzhe, JIN Jianghong. Summary of integrated application of functional safety and information security in industry[C]// *2018 12th International Conference on Reliability, Maintainability, and Safety (ICRMS)*. Shanghai, China: IEEE, 2018: 463-469.
- [36] ŚLIWIŃSKI M, PIESIK E, PIESIK J. Integrated functional safety and cyber security analysis[J]. *IFAC-PapersOnLine*, 2018, 51(24): 1263-1270.
- [37] MODI C, PATEL D, BORISANIYA B, et al. A survey of intrusion detection techniques in Cloud[J]. *Journal of Network and Computer Applications*, 2013, 36(1): 42-57.
- [38] 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(1): 53-60.  
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.
- [39] KRIAA S, PIETRE-CAMBACÉDES 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.
- [40] ZHONG R Y, XU Xun, KLOTZ E, et al. Intelligent manufacturing in the context of industry 4.0: a review[J]. *Engineering*, 2017, 3(5): 616-630.
- [41] 安成飞, 等. 保 2.0 下工业控制系统安全防护[J]. *自动化博览*, 2019, 36(S2): 102-105.  
AN Chengfei. Security protection of industrial control system under classified protection of cybersecurity 2.0[J]. *Automation Panorama*, 2019, 36(S2): 102-105.
- [42] 宫敬, 徐波, 张微波. 中俄东线智能化工艺运行基础与实现的思

- 考[J]. 油气储运, 2020, 39(2): 130-139.
- GONG Jing, XU Bo, ZHANG Weibo. Thinking on the basis and realization of intelligent process operation of China-Russia eastern gas pipeline[J]. Oil & Gas Storage and Transportation, 2020, 39(2): 130-139.
- [43] 王子宗, 高立兵, 索寒生. 未来石化智能工厂顶层设计: 现状、对比及展望[J]. 化工进展, 2022, 41(7): 3387-3401.
- WANG Zizong, GAO Libing, SUO Hansheng. Designing petrochemical smart plant of the future: state of the art, comparison and prospects[J]. Chemical Industry and Engineering Progress, 2022, 41(7): 3387-3401.
- [44] 胡旭光. 基于随机矩阵谱理论的成品油管道管网故障诊断方法研究[D]. 沈阳: 东北大学, 2017.
- HU Xuguang. Research on products oil pipeline network fault diagnosis based on spectral theory of random matrix[D]. Shenyang: Northeastern University, 2017.
- [45] 孟祥坤, 陈国明, 朱红卫. 海底管道泄漏风险演化复杂网络分析[J]. 中国安全生产科学技术, 2017, 13(4): 26-32.
- MENG Xiangkun, CHEN Guoming, ZHU Hongwei. Complex network analysis on risk evolution of submarine pipeline leakage[J]. Journal of Safety Science and Technology, 2017, 13(4): 26-32.
- [46] 卢绍文, 张超. 某酸浸冶炼生产物理信息系统的复杂网络特征[J]. 复杂系统与复杂性科学, 2016, 13(3): 81-85.
- LU Shaowen, ZHANG Chao. Complex topology features of the cyber physical system of an acid leaching industrial process[J]. Complex Systems and Complexity Science, 2016, 13(3): 81-85.
- [47] DING Kai, LEI Jingyuan, ZHANG Fuqiang, et al. Analyzing the cyber-physical system-based autonomous collaborations among smart manufacturing resources in a smart shop floor[J]. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 2020, 234(3): 489-500.
- [48] WEI Yongsong, LI Shaoyuan. Water supply networks as cyber-physical systems and controllability analysis [J]. IEEE/CAA Journal of Automatica Sinica, 2015, 2(3): 313-319.
- [49] 陈世明, 邹小群, 吕辉, 等. 面向级联失效的相依网络鲁棒性研究[J]. 物理学报, 2014, 63(2): 028902.
- CHEN Shiming, ZOU Xiaoqun, LÜ Hui, et al. Research on robustness of interdependent network for suppressing cascading failure[J]. Acta Physica Sinica, 2014, 63(2): 028902.
- [50] HUANG Zhen, WANG Cheng, NAYAK A, et al. Small cluster in cyber physical systems: network topology, interdependence and cascading failures [J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(8): 2340-2351.
- [51] 董政呈. 相互依存网络的抗毁性研究及在电力系统的应用[D]. 武汉: 武汉大学, 2016.
- DONG Zhengcheng. Research on the invulnerability of interdependent networks and its applications in power system[D]. Wuhan: Wuhan University, 2016.
- [52] 蒋将. 基于网络科学的复杂电力系统建模与分析[D]. 杭州: 浙江大学, 2021.
- JIANG Jiang. Modeling and analysis of complex power system based on network science[D]. Hangzhou: Zhejiang University, 2021.
- [53] XU Luo, GUO Qinglai, YANG Tianyu, et al. Robust routing optimization for smart grids considering cyber-physical interdependence[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5620-5629.
- [54] 冀星沛, 王波, 刘涤尘, 等. 相依网络理论及其在电力信息-物理系统结构脆弱性分析中的应用综述[J]. 中国电机工程学报, 2016, 36(17): 4521-4532.
- JI Xingpei, WANG Bo, LIU Dichen, et al. Review on interdependent networks theory and its applications in the structural vulnerability analysis of electrical cyber-physical system[J]. Proceedings of the CSEE, 2016, 36(17): 4521-4532.
- [55] GUO Jia, HAN Yuqi, GUO Chuangxin, et al. Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties[J]. Energies, 2017, 10(1): 87.
- [56] ILIC M D, XIE Le, KHAN U A, et al. Modeling of future cyber-physical energy systems for distributed sensing and control[J]. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 2010, 40(4): 825-838.
- [57] NOURIAN A, MADNICK S. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(1): 2-13.
- [58] 曹科宁, 李仁发, 张小明, 等. 面向 CPS 复杂事件流的不确定性研究[J]. 计算机工程与科学, 2015, 37(3): 415-421.
- CAO Kening, LI Renfa, ZHANG Xiaoming, et al. Research on uncertain CEP for CPS[J]. Computer Engineering & Science, 2015, 37(3): 415-421.
- [59] 江奕勋, 张立臣. 基于信息物理融合系统的时空建模方法[J]. 现代计算机, 2020(25): 32-36.
- JIANG Yixun, ZHANG Lichen. Space-time modeling method based on information physics fusion system[J]. Modern Computer, 2020(25): 32-36.
- [60] 许亮, 刘兰英, 李秀喜. 面向化工过程安全运行的信息物理融合系统[J]. 现代化工, 2016, 36(3): 169-172.
- XU Liang, LI Lanying, LI Xiuxi. Cyber-physical system for safe operation of chemical processes[J]. Modern Chemical Industry, 2016, 36(3): 169-172.
- [61] 王云. 基于混合系统的主动配电网信息物理融合建模与控制[D]. 上海: 上海交通大学, 2017.
- WANG Yun. Cyber physical system integration modeling and control for active distribution network based on hybrid system [D]. Shanghai: Shanghai Jiao Tong University, 2017.
- [62] 王云, 刘东, 陆一鸣. 电网信息物理系统的混合系统建模方法研究[J]. 中国电机工程学报, 2016, 36(6): 1464-1470.
- WANG Yun, LIU Dong, LU Yiming. Research on hybrid system modeling method of cyber physical system for power grid[J]. Proceedings of the CSEE, 2016, 36(6): 1464-1470.
- [63] 王云, 刘东, 翁嘉明, 等. 电网信息物理系统建模与仿真验证平台研究[J]. 中国电机工程学报, 2018, 38(1): 130-136.
- WANG Yun, LIU Dong, WENG Jiaming, et al. The research of power CPS modeling and simulation verification platform [J]. Proceedings of the CSEE, 2018, 38(1): 130-136.
- [64] ZHU Yufeng, DONG Yunwei, MA Chunyan, et al. A methodology of model-based testing for AADL flow latency in CPS[C]// 2011 5th International Conference on Secure Software Integration & Reliability Improvement Companion (SSIRI-C). Jeju, South Korea: IEEE, 2011: 99-105.
- [65] SUN Zhonghao, ZHOU Xingshe. Extending and recompiling AADL

- for CPS modeling[C]//2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China; IEEE, 2013; 1225-1230.
- [66] ZHANG Lichen. Specifying and modeling automotive cyber physical systems[C]//2013 IEEE 16th International Conference on Computational Science and Engineering (CSE). Sydney, Australia; IEEE, 2013; 603-610.
- [67] ZHANG Lichen. An integration approach to specify and model automotive cyber physical systems[C]//2013 International Conference on Connected Vehicles and Expo (ICCVE). Las Vegas, USA; IEEE, 2013; 568-573.
- [68] GUAN Tao, YANG Gang. Integration-oriented modeling of cyber-physical interactive process[C]//2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China; IEEE, 2013; 1492-1495.
- [69] ZHANG Lichen. Multi-dimensional analysis and design method for aerospace cyber-physical systems[C]//2013 12th International Symposium on Distributed Computing and Applications to Business, Engineering & Science. Kingston upon Thames, UK; IEEE, 2013; 197-201.
- [70] 赵福迪, 柳先辉. 信息物理融合系统建模技术研究[J]. 信息技术, 2021, 45(9): 1-6.  
ZHAO Fudi, LIU Xianhui. Research on modeling technology of cyber-physics fusion system[J]. Information Technology, 2021, 45(9): 1-6.
- [71] MANSOORI M, WELCH I, CHOO K K R, et al. Application of HAZOP to the design of cyber security experiments[C]//IEEE 30th International Conference on Advanced Information Networking & Applications. Crans-Montana, Switzerland; IEEE, 2016; 790-799.
- [72] UMEDA H, NAMIHIRA K, OKUBO N, et al. FMEA focusing on the interaction between physical and computational elements in cyber-physical systems[C]//2021 Annual Reliability and Maintainability Symposium (RAMS). Orlando; IEEE, 2021; 1-7.
- [73] TANTAWY A, ERRADI A, ABDELWAHED S. A modified layer of protection analysis for cyber-physical systems security[C]//2019 4th International Conference on System Reliability and Safety (IC-SRS). Rome, Italy; IEEE, 2019; 94-101.
- [74] CARRERAS GUZMAN N H, KOZINE I, LUNDTEIGEN M A. An integrated safety and security analysis for cyber-physical harm scenarios[J]. Safety Science, 2021, 144: 105458.
- [75] 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.
- [76] TANTAWY A, ABDELWAHED S, ERRADI A, et al. Model-based risk assessment for cyber physical systems security[J]. Computers & Security, 2020, 96: 101864.
- [77] 韩宇奇, 郭创新, 朱炳铨, 等. 基于改进渗流理论的信息物理融合电力系统连锁故障模型[J]. 电力系统自动化, 2016, 40(17): 30-37.  
HAN Yuqi, GUO Chuangxin, ZHU Bingquan, et al. Model cascading failures in cyber physical power system based on improved percolation theory[J]. Automation of Electric Power Systems, 2016, 40(17): 30-37.
- [78] 邓勇, 彭敏放, 刘靖雯. 电力信息物理系统建模和信息攻击机制分析[J]. 电力系统及其自动化学报, 2021, 33(10): 10-17.  
DENG Yong, PENG Minfang, LIU Jingwen. Modeling of cyber power physical system and analysis of information attack mechanism[J]. Proceedings of the CSU-EPSA, 2021, 33(10): 10-17.
- [79] 翁嘉明, 刘东, 安宇, 等. 馈线功率控制下的主动配电网信息物理风险演化分析[J]. 中国电力, 2021, 54(3): 13-22.  
WENG Jiaming, LIU Dong, AN Yu, et al. Cyber-physical risk evolution analysis of active distribution network under feeder control error[J]. Electric Power, 2021, 54(3): 13-22.
- [80] KWON C, HWANG I. Reachability analysis for safety assurance of cyber-physical systems against cyber attacks[J]. IEEE Transactions on Automatic Control, 2018, 63(7): 2272-2279.
- [81] VERMA S, GRUBER T, SCHMITTNER C, et al. Combined approach for safety and security[C]//SAFECOMP 2019 Workshops on Computer Safety, Reliability, and Security. Turku, Finland; Springer, 2019; 87-101, doi: 10.1007/978-3-030-26250-1\_7.
- [82] LIU Xiaoxue, ZHANG Jiexin, ZHU Peidong. Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory[J]. International Journal of Critical Infrastructure Protection, 2017, 16: 13-25.
- [83] THRAMBOULIDIS K, CHRISTOULAKIS F. UML4IoT—A UML-based approach to exploit IoT in cyber-physical manufacturing systems[J]. Computers in Industry, 2016, 82: 259-272.
- [84] THRAMBOULIDIS K. A cyber-physical system-based approach for industrial automation systems[J]. Computers in Industry, 2015, 72: 92-102.
- [85] TORKILDSON E N, LI Jingyue, JOHNSEN S O, et al. Empirical studies of methods for safety and security co-analysis of autonomous boat[M]//HAUGEN S, BARROS A, GULIJK C, et al. Safety and Reliability-Safe Societies in A Changing World. London; CRC Press, 2018.
- [86] KORNECKI A J, SUBRAMANIAN N, ZALEWSKI J. Studying interrelationships of safety and security for software assurance in cyber-physical systems; approach based on Bayesian belief networks[C]//2013 Federated Conference on Computer Science and Information Systems. Krakow, Poland; IEEE, 2013; 1393-1399.
- [87] 周明, 吕世超, 游建舟, 等. 工业控制系统安全态势感知技术研究[J]. 信息安全学报, 2022, 7(2): 101-119.  
ZHOU Ming, LÜ Shichao, YOU Jianzhou, et al. A comprehensive survey of security situational awareness on industrial control systems[J]. Journal of Cyber Security, 2022, 7(2): 101-119.
- [88] BASU C, PADMANABAN M, GUILLON S, et al. Situational awareness for the electrical power grid[J]. IBM Journal of Research and Development, 2016, 60(1): 10: 1-10; 11.
- [89] 张小俊, 史威, 贾立东, 等. 工业网络安全态势感知平台在能源管道行业应用的机遇与挑战[J]. 自动化应用, 2021(8): 80-82.  
ZHANG Xiaojun, SHI Wei, JIA Lidong, et al. Opportunities and challenges of industrial network security situational awareness platform application in energy pipeline industry[J]. Automation Application, 2021(8): 80-82.
- [90] WANG Yong, XU Zhaoyan, ZHANG Jialong, et al. SRID: state relation based intrusion detection for false data injection attacks in SCADA[C]//19th European Symposium on Research in Computer Security. Wroclaw, Poland; Springer, 2014; 401-418.

- South China Sea[J]. *Acta Sedimentologica Sinica*, 2010, 28(5): 987-1005.
- [21] 张功成, 苗顺德, 陈莹, 等. “源热共控”中国近海天然气富集区分布[J]. *天然气工业*, 2013, 33(4): 1-17.  
ZHANG Gongcheng, MIAO Shunde, CHEN Ying, et al. Distribution of gas enrichment regions controlled by source rocks and geothermal heat in China offshore basins[J]. *Natural Gas Industry*, 2013, 33(4): 1-17.
- [22] 张功成, 陈国俊, 张厚和, 等. “源热共控”中国近海盆地油气田“内油外气”有序分布[J]. *沉积学报*, 2012, 30(1): 1-19.  
ZHANG Gongcheng, CHEN Guojun, ZHANG Houhe, et al. Regular distribution of inside-oil fields and outside-gas fields controlled by source rocks and heat in China offshore basins[J]. *Acta Sedimentologica Sinica*, 2012, 30(1): 1-19.
- [23] 于翠玲, 李宝刚. 渤海湾盆地东营凹陷牛庄洼陷岩性油气藏平面富集主控因素[J]. *吉林大学学报: 地球科学版*, 2019, 49(1): 240-247.  
YU Cuiling, LI Baogang. Main factors controlling planar enrichment of lithologic reservoirs in Niuzhuang sub-sag, Dongying depression, Bohai Bay Basin[J]. *Journal of Jilin University: Earth Science Edition*, 2019, 49(1): 240-247.
- [24] 吕延防, 付广, 付晓飞, 等. 断层对油气的输导与封堵作用[M]. 北京: 石油工业出版社, 2013.  
LÜ Yanfang, FU Guang, FU Xiaofei, et al. Transporting and sealing effect of faults[M]. Beijing: Petroleum Industry Press, 2013.
- [25] 李明诚. 石油与天然气运移[M]. 4版. 北京: 石油工业出版社, 2013.  
LI Mingcheng. Oil and gas migration[M]. 4th ed. Beijing: Petroleum Industry Press, 2013.
- [26] 朱俊章, 施洋, 熊万林, 等. 开平凹陷古近系稠油和砂岩储层沥青质成因分析[J]. *中国海上油气*, 2020, 32(2): 34-43.  
ZHU Junzhang, SHI Yang, XIONG Wanlin, et al. Genesis analysis of Paleogene heavy oil and asphaltene in sandstone reservoir in Kaiping sag[J]. *China Offshore Oil and Gas*, 2020, 32(2): 34-43.
- [27] 郭雪. 断裂在盖层段的变形机制及垂向封闭能力[D]. 大庆: 东北石油大学, 2012.  
GUO Xue. Deformation mechanism of fracture in the cap rock and vertical sealing ability [D]. Daqing: Northeast Petroleum University, 2012.
- [28] 陈美伊. 断裂在不同脆韧性泥岩盖层内垂向封闭性评价方法研究[D]. 大庆: 东北石油大学, 2020.  
CHEN Meiyi. Research on the evaluation method of vertical sealing ability of faults in mudstone cap-rock of different brittleness [D]. Daqing: Northeast Petroleum University, 2020.
- [29] 鲁雪松, 柳少波, 田华, 等. 深层背斜圈闭中泥岩盖层完整性评价方法及其应用——以四川盆地川中地区震旦系气藏为例[J]. *石油学报*, 2021, 42(4): 415-427.  
LU Xuesong, LIU Shaobo, TIAN Hua, et al. An evaluation method for the integrity of mudstone caprock in deep anticlinal traps and its application: a case study of the Sinian gas reservoirs in the central Sichuan Basin[J]. *Acta Petrolei Sinica*, 2021, 42(4): 415-427.
- [30] 张昊天, 周文, 曹茜, 等. 基于应力—应变模型的脆塑性测井评价[J]. *测井技术*, 2018, 42(3): 331-337.  
ZHANG Haotian, ZHOU Wen, CAO Qian, et al. Log evaluation method of the brittle-plastic parameters based on stress-strain model[J]. *Well Logging Technology*, 2018, 42(3): 331-337.
- [31] 李颜辰. 砂-泥互层地层断裂带内部结构特征[D]. 大庆: 东北石油大学, 2017.  
LI Yanchen. Internal structure characteristics of fault zones in sand-mud interbedded formations[D]. Daqing: Northeast Petroleum University, 2017.
- [32] 付晓飞, 郭雪, 朱丽旭, 等. 泥岩涂抹形成演化与油气运移及封闭[J]. *中国矿业大学学报*, 2012, 41(1): 52-63.  
FU Xiaofei, GUO Xue, ZHU Lixu, et al. Formation and evolution of clay smear and hydrocarbon migration and sealing[J]. *Journal of China University of Mining & Technology*, 2012, 41(1): 52-63.

(收稿日期 2022-06-28 改回日期 2023-03-21 编辑 宋宁)

(上接第 916 页)

- [91] CHIEN D. Systems and methods for suppressing denial of service attacks; US, 10277626B2[P]. 2019-04-30.
- [92] 陆耿虹, 冯冬芹. 基于改进 C-SVC 的工控网络安全态势感知[J]. *控制与决策*, 2017, 32(7): 1223-1228.  
LU Genghong, FENG Dongqin. Industrial control network security situation awareness based on improved C-SVC[J]. *Control and Decision*, 2017, 32(7): 1223-1228.
- [93] 罗涛, 孙阔, 张章, 等. 多能源数据驱动的电力信息物理系统综合态势感知模型[J]. *可再生能源*, 2021, 39(3): 395-400.  
LUO Tao, SUN Kuo, ZHANG Zhang, et al. Comprehensive situation awareness model of power cyber-physical system driven by multi-energy data[J]. *Renewable Energy Resources*, 2021, 39(3): 395-400.
- [94] IAIANI M, TUGNOLI A, MACINI P, et al. Outage and asset damage triggered by malicious manipulation of the control system in process plants[J]. *Reliability Engineering & System Safety*, 2021, 213: 107685.
- [95] 张世斌, 贾立东, 魏义昕, 等. 输气管道 SCADA 系统网络安全策略探索与实现——以中俄东线天然气管道工程为例[J]. *油气储运*, 2020, 39(6): 685-691.  
ZHANG Shibin, JIA Lidong, WEI Yixin, et al. Exploration and implementation of network security strategy for gas pipeline SCADA system: taking the China-Russia Eastern Gas Pipeline Project as an example[J]. *Oil & Gas Storage and Transportation*, 2020, 39(6): 685-691.
- [96] NING Xirong, JIANG Jin. Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems[J]. *IEEE Transactions on Industrial Informatics*, 2022, 18(2): 1154-1164.

(收稿日期 2022-12-04 改回日期 2023-03-24 编辑 王培玺)