中文引用格式:牛莉霞,李肖萌,王洪妹. 5G时代负系统学视域下智能系统安全分析体系构建[J]. 中国安全科学学报,2024,34(8):1-10.

英文引用格式:NIU Lixia, LI Xiaomeng, WANG Hongmei. Construction of intelligent system security analysis system under view of negative systematics in 5G era[J]. China Safety Science Journal, 2024, 34(8): 1-10.

5G时代负系统学视域下智能系统安全分析体系构建*

牛莉霞 教授, 李肖萌, 王洪妹

(辽宁工程技术大学 工商管理学院,辽宁 葫芦岛 125105)

中图分类号:X913 **文献标志码**:A **DOI**: 10.16265/j.cnki.issn1003-3033.2024.08.0226

基金项目:国家自然科学基金资助(52174184);辽宁省社科联项目(2023lslybkt-072)。

【摘 要】 为探究安全事故的负面性与普遍性,首先,依据安全科学的负系统学逆向思维范式,结合系统科学的生态系统理论,确定智能系统开放包容性、交互耦合性、动态平衡性特性,明晰智能系统安全分析逻辑理路;然后,从负系统学视角切入,确定安全事故危险源,阐述安全事故产生机制,引入内聚耦合概念,提出s型框架模型,用于分析智能系统子系统稳定性,探究其底层技术支持;最后,利用生产者、传播者、消费者、分解者概念,分析智能系统信息流动全过程动态平衡,共同形塑负系统学视域下智能系统安全分析体系。结果表明:所建立的负系统学视域下智能系统安全分析框架体系,能够有效分析智能系统的安全稳定运行及信息流动全过程的动态平衡,确保智能系统安全分析的全面性和可靠性。

【关键词】 5G时代; 负系统学; 智能系统; 安全分析; 生态系统理论

Construction of intelligent system security analysis system under view of negative systematics in 5G era

NIU Lixia, LI Xiaomeng, WANG Hongmei

(School of Business Management, Liaoning Technical University, Huludao Liaoning 125105, China)

Abstract: In order to explore the negativity and universality of security incidents, a reverse thinking paradigm based on Negative Systems Theory in safety science was first applied in conjunction with the Ecosystem Theory from systems science. This approach identified the characteristics of intelligent systems—openness, inclusivity, interactive coupling, and dynamic balance—and clarified the logical framework for intelligent system security analysis. Subsequently, the sources of security incident hazards were identified from the perspective of negative systems theory, and the mechanisms behind security incidents were explained. The concept of cohesive coupling was introduced, and an s-shaped framework model was proposed to analyze the stability of subsystems within intelligent systems and investigate their underlying technological support. Finally, using the concepts of producers, transmitters, consumers, and decomposers, the dynamic balance of information flow throughout the entire process in intelligent systems was analyzed, collectively shaping the security analysis framework under the negative systems theory

* 文章编号:1003-3033(2024)08-0001-10; 收稿日期:2024-02-16; 修稿日期:2024-05-20

perspective. The results indicated that the security analysis framework established under the negative systems theory perspective could effectively analyze the secure and stable operation as well as the dynamic balance of information flow throughout intelligent systems, ensuring the comprehensiveness and reliability of intelligent system security analysis.

Keywords: 5G era; negative systematics; intelligent systems; security analysis; ecosystem theory

0 引　言

对企业智能系统进行正确地安全分析,并不断优化提升其安全性能,有助于促进企业的长期稳定和快速发展[1]。伴随5G时代的到来及数据驱动思维的影响,智能系统逐渐成为子系统、技术和信息构成的复杂集合体[2-3],系统的重心从物理空间向信息空间转移,并具备类似生态系统的“自组织、自生长、自适应和自修正”特性。传统的安全分析方法难以有效地应对智能系统的复杂性与动态性。因此,迫切需要更加逻辑化、系统化和科学化的分析方法,以确保智能系统安全分析的全面性和可靠性。

智能系统在终端应用中呈现出多样化的形态,涉及多元信息主体且关系复杂,众多子系统间协同交互以提供综合服务[4],与此同时,系统运行支持技术日新月异,高新技术不断涌现[5]。这些因素使智能系统多形态基础设施、全生命流程的动态监管与安全防控工作变得更加复杂[6-8]。当前,智能系统的安全分析主要围绕生产流程[9]、安全事故[10]、数据要素[11]、高新技术[12]等开展,但尚未形成全面完善的安全分析体系。而且,在现有智能系统安全分析过程中,相关研究的指导思想、基础理论、研究方法和范式等都处于相对分裂的状态。因此,亟需建立一个统一的思维范式,并在此基础上开展系统性的智能系统安全分析研究。

鉴于此,笔者采用负系统学思维范式,结合成熟的生态系统理论,基于智能系统的生态特性,确定智能系统安全分析流程。通过深入分析智能系统的子系统与技术支持的安全稳定运行,并探讨运行过程中信息流动的全过程动态平衡,以期建立一个系统化的智能系统安全分析体系。

1 智能系统安全分析体系构建思路

1.1 智能系统安全分析特性

1) 系统化安全分析。5G时代,智能系统通常由多个子系统构成,整体运维流程更加繁琐,相较于以往更为复杂化、信息化、智能化[13-14]。因此,需要一个系统化的智能系统安全分析方案,以确保各子系统功能的实现。

2) 动态安全分析。智能系统在日常运维过程中长期处于动态稳定状态,传统的静态、片面的安全分析方法显然已不足以应对智能系统复杂的安全问题。因此,从静态分析延伸到动态分析是智能系统安全分析的必经之路。

3) 引入信息流参与系统安全分析。随着数字技术的发展,数据逐渐成为新型生产要素,并在智能系统中扮演愈发重要的角色[15]。信息作为数据的载体,流通是否通畅成为智能系统分析的重要评价标准[16]。

4) 多学科相互碰撞。智能系统作为复杂系统,结合了计算机科学、数学、工程学、物理学、认知科学、生物学等多种学科的知识与技术,因此智能系统的安全分析同样离不开多学科理论的交叉融合[17]。

1.2 智能系统安全分析思维

1) 负系统学思维。吴超[17]将负系统定义为在特定时空和环境条件下,由若干相互关联又相互矛盾的负组分共同演化出负面结果的统一体。负组分由负元素集合而成,这些负元素的具体化形态(负元人、负元事、负元物、负元信息)在事件演化过程中相互耦合,最终导致安全事故的发生[18-19]。安全事故是系统中涌现出的人们不希望发生的事件。一般而言,安全事故的后果是显性的、可观测的,但是随着安全系统内涵的不断延伸,没有事故发生并不代表系统处于良好状态。系统中可能存在部分隐性不安全状态,但这些状态没有达到负元素的涌现阈值。因此,对智能系统的安全分析应拓展到对负元素数据的实时观测。即使负元素的状态尚未达到导致事故的阈值,也应全流程监测负元素数据,以期达到预防安全系统隐性事故的效果。

2) 生态系统理论。ARTHUR[20]于1935年首次提出生态系统(Ecosystem)概念,认为生态系统是在一定时间和空间范围内,各元素通过物质循环、信息传递和能量流动形成的特定结构和功能单位。在

学术界,生态系统理论已被广泛应用于各种复杂系统,并逐渐形成信息生态学[21]、创新生态学[22]等多种分支学科。笔者从负系统学视角开展研究,结合生态系统理论,使复杂智能系统的安全分析更加全面系统。

3) 负系统学视角下智能系统安全生态分析。作为一种复杂系统,负系统学视域下,智能系统的系统表达与生物学意义上的生态系统具有一定的相似性与相关性,如图 1 所示。

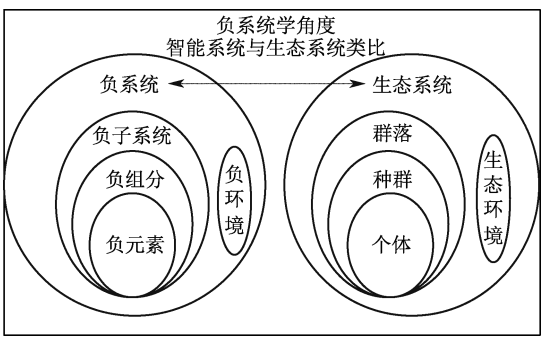

图 1　负系统学视角下智能系统与生态系统类比分析

Fig. 1　Analogical analysis of intelligent systems and ecosystems from a negative systematics perspective

从生物学视角来看,生态系统由个体、种群、群落到生态系统,层层递进,具有物质循环、能量流动和信息流动的特征。从负系统学角度出发分析智能系统可以发现,智能系统中各种负元素构成了负组分,负组分聚合构成负子系统,负子系统与负环境相耦合,最终形成负系统。与此同时,类似于生态系统,智能系统中的物质、能量、信息也在系统内循环流动,各种负元素处于一种微妙的动态平衡。因此,在负系统学思维模式下,智能系统与生态系统的结构构成和动态平衡之间存在巧妙的相似性。

鉴于此,可以归纳出,一个安全稳定的智能系统应具备开放包容性、交互耦合性和动态平衡性这 3 个特性。①开放包容性。在稳定运行状态下,智能系统主体持续与环境持续进行知识、技术和信息的互动和交换。开放包容性是智能系统安全分析的基础,确保智能系统与外部环境的稳定联系和交换,从而保障系统整体功能与性能的实现。②交互耦合性。智能系统的各组成部分之间相互作用、紧密耦合,这些互动直接决定了系统的整体性能、响应速度、稳定性和适应性。通过优化和增强这些交互耦合关系,智能系统可以更好地发挥其预期功能,提升在复杂环境下的操作性能,进而达到更高的智能化水平。③动态平衡性。智能系统的动态平衡性是指系统在不断变化的环境中,能够保持自身稳定运行并适应外部变化的能力。这一特性对于智能系统的设计与运行至关重要,它决定了系统在遭遇复杂和不可预测的外部环境时,是否能够维持高效运作和准确响应。

1.3　智能系统安全分析流程

5G 时代,智能系统的开放包容性在安全分析中扮演着根本性的角色。正是依托于这种开放包容性,智能系统内外部元素与环境持续互动,适应不同的数据源、技术、应用场景和外部环境,并实现与其他系统或组件的互操作和集成。智能系统的开放包容性不仅是其功能强大和广泛适应性的基础,也是开展全面和有效安全分析的基础。

因此,笔者以智能系统的开放包容性为基础,根据智能系统的交互耦合性和动态平衡性,结合智能系统所处自然环境、社会环境、政策环境、文化环境的变化,探讨智能系统是否能够通过系统和功能的耦合实现智能系统的自适应,自稳定、自决策、自优化,同时,分析整个管理体系是否处于一种巧妙的动态平衡状态。智能系统安全分析具体流程如图 2 所示。

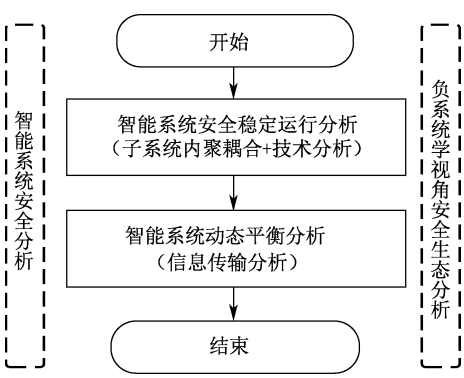

图 2　智能系统安全分析流程

Fig. 2　Intelligent system security analysis process

首先,考察智能系统子系统内聚耦合程度,探究各子系统间的协同水平以及各元素的独立性,进而分析整个智能系统的稳定性。同时,系统稳定是实现其功能的前提,而高新技术的支持则是确保系统稳定运行的关键,因此有必要对智能系统进行技术支持分析。

然后,检查智能系统信源是否准确无误、信道是否畅通无阻,以探究智能系统的动态平衡性。确保信息准确、快速的传递以及安全信息流的通畅是维持智能系统安全动态平衡必不可少的条件。

最后,根据事故全过程理论,分析智能系统在安全信息的采集、处理、使用、销毁等过程中的表现,探究智

能系统的态势感知—风险评估与预测—情景分析能力,综合评判智能系统风险应对能力,确保智能系统能够精准预防风险,快速响应事故,从而在复杂多变的环境中维持动态平衡,确保系统的安全稳定运行。

2 智能系统安全稳定运行分析

2.1 智能系统事故产生机制分析

智能系统是复杂系统,由物质、能量、信息及其之间的关联关系构成[23-25]。在生态系统中,食物链和食物网构成了物种间的营养关系;而在智能系统中,信息流、能量流、物质流维系着整个系统的稳定。根据事故致因能量学说,傅贵等[26]认为,可能导致事故的能量和物质被视为事故的危险源,阻止物质或者能量不正常传递的事物被称为屏障。在5G时代,信息流作为物质流和能量流的表征,在安全事故发生过程中不可忽视[27]。据此,笔者分析了智能系统安全事故产生机制,如图3所示。

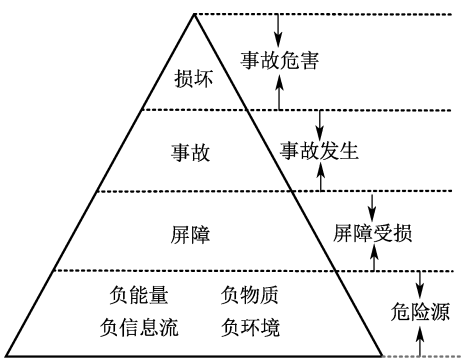

图3 智能系统安全事故产生机制

Fig. 3 Mechanisms for generating security incidents in intelligent systems

在常态情况下,系统内外保持稳定,各元素正常发挥功能;在非常态条件下,如果危险源屏障失效,大量负能量和负物质涌现,导致事故发生。因此,智能系统的稳定运行状态下各负元素均低于阈值,且各子系统保持安全稳定运行状态。

2.2 智能系统交互耦合稳定性分析

元素、信息和环境相互作用,共同维持智能系统的稳定运行。在5G时代背景下,智能系统通过各子系统的协作与交互联结构成,其内部各负元素的状态直接决定了智能系统的稳定性。

文中引入内聚、耦合概念,用于度量智能系统中各子系统的关联度[28],并提出s型内聚耦合理论,如图4所示。

在智能系统内用内聚度来度量系统中各元素自

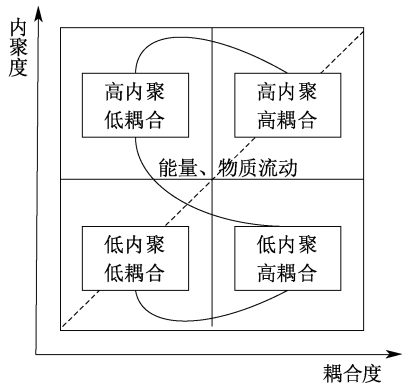

图4 s型内聚耦合

Fig. 4 s-type cohesive coupling

运行程度,内聚度越高,元素越独立,越不易受到环境等其它因素的影响;耦合度用来度量各智能子系统间的协同程度,耦合度越高各子系统联系越紧密,各子系统协同效用越强,独立性越差,其中任一子系统发生微小变化,都将带动其余子系统纷纷产生动荡,容易导致安全事故的产生。关于智能系统内聚耦合性分类情况具体说明如下:

1)低内聚、低耦合(各人自扫门前雪)。在此状态下,智能系统中各元素虽然独立运行,不会互相影响,但其功能性较弱,无法形成协同作用。此种状态下,系统的整体效率较低,虽然独立性高,但缺乏有效的功能结构。

2)低内聚、高耦合(一盘散沙)。该象限表示系统内部结构混乱,各元素功能散乱,且子系统间的过度耦合使得系统脆弱且容易出问题。这个状态通常是系统设计中应避免的,因为不仅效率低下,而且极易导致系统崩溃。

3)高内聚、低耦合(各司其职)。在这个象限中,智能系统中各元素功能分明,各司其职,形成一个高效的系统。系统内各子系统独立运行,即使某一部分出现问题,整体系统依然能保持稳定。此状态是智能系统安全管理的理想状态。

4)高内聚、高耦合(牵一发而动全身)。在这个象限中,虽然各元素内部功能性强,但由于各子系统之间联系过于紧密,一个子系统的负面效应可能引发整个系统的不稳定。此状态可能存在潜在的风险,尽管系统运行效率高,但其鲁棒性较差。

图中s型曲线代表智能系统从低内聚、低耦合状态(低效和脆弱)逐渐优化,经历不同阶段,向高内聚、低耦合状态(高效和稳健)发展的过程。这提示管理者在智能系统管理过程中应努力提升其内聚性,同时,适度控制耦合性,内紧而外松,使系统内部

各元素高度聚合,产生巨大向心力,又能围绕目标各司其职,各子系统独立完成任务,以期实现一个高效且稳定的智能系统。

2.3　智能系统稳定运行技术支持分析

智能系统运行安全的本质在于利用数智化高新技术,提升其应对外部干扰和内部故障的能力,从而增强整体系统的高效性、安全性和协同运作能力,确保智能系统的安全稳定运行[29-30]。

5G 时代,全面的技术支持是确保智能系统稳定运行的核心保障,也是推动中国式安全管理现代化的关键因素。在智能系统中,人员、技术、环境、管理子系统紧密相连,通过分析类、传输类、感知类和应用类高新技术交叉融合。这些子系统协同作用,共同促进智能系统安全生态循环,保障系统整体的安全性与稳定性。笔者按照信息数据的获取、传输及应用路径分析智能系统各保障子系统高新技术,如图 5 所示。

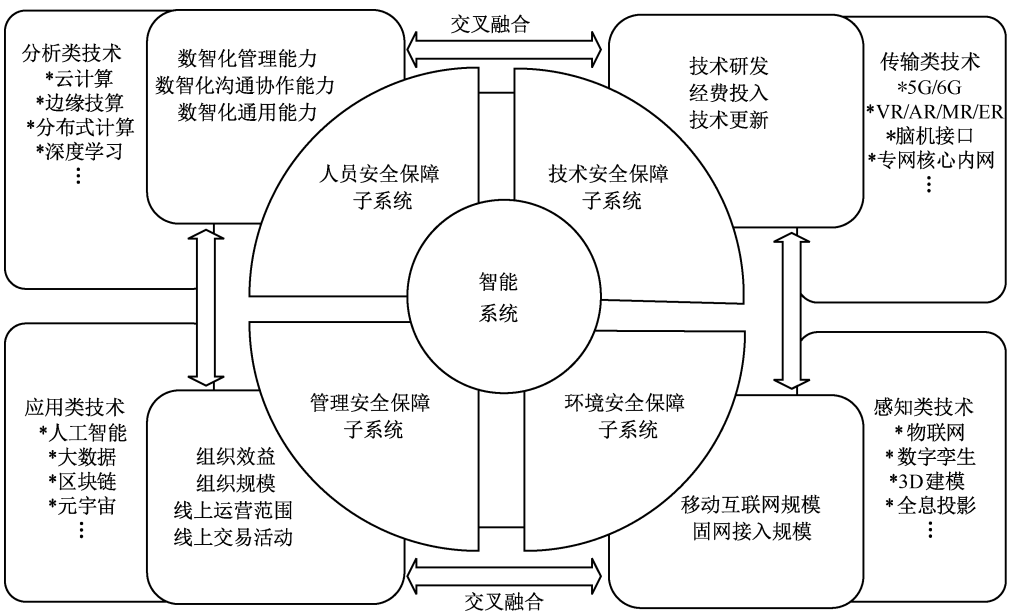

图 5　智能系统子系统技术支持运行分析

Fig. 5　Analysis of technical support operation for subsystems of intelligent system

1) 感知类技术。感知类技术是智能系统获取外界和内部信息的主要手段,主要包括物联网技术、数字孪生等虚拟现实技术。这些技术通过将智能系统的物理场景与虚拟场景相互映射,打破时间、空间局限,实现智能系统的全方位安全感知、高广度覆盖和深度沉浸。它们形成全域、全时段、全流程的监控子系统,可用于构建一个全景式的智慧应急新场景。

分析感知类技术时,应重点关注传感器可能遭受的篡改与欺骗攻击、数据完整性、环境干扰以及隐私保护等问题。通过精准控制移动互联网、固网等接入的规模,将虚拟场景与真实场景叠加、重构,以虚控实,可以对智能系统环境子系统中负元素的涌现进行持续性观测,从而保障数据的真实性和完整性。

2) 传输类技术。借助 5G 网络的大流量传输优势,通过专网、核心内网、脑机接口等技术,执行安全扫描并传递安全信息。同时,利用触觉互联网对智能系统中的数据信息进行扫描与传输,为智慧应急和风险预警提供决策依据。

分析传输类技术时,应重点关注技术应用过程中可能发生的数据泄露、篡改和拦截风险,加强传输数据的加密、实施用户身份认证与访问控制等问题,确保网络安全以及数据传输的完整性。同时,应保证对传输类技术的经费投入与技术研发,相关部门应定期组织巡查,监控高新技术使用情况,并对技术更新情况进行记录与分析,以保障智能系统中技术子系统感知信息的稳定传输。

3) 分析类技术。分析类技术主要包括云计算、边缘技术、深度学习等,通过高性能计算技术优化智能系统的算力,对采集到的安全信息进行分析计算,观测负元素涌现,并提升安全信息刻画效果,从而为智能系统的安全分析和决策提供坚实依据。

在分析类技术的评估中,应重点关注算法的安全性、数据保护与隐私维护、抵御恶意数据注入,以及保证模型的完整性与安全性。确保分析类技术的实施符合数据隐私和安全要求,同时提供加密、访问控制等技术支持。此外,应针对技术人员和最终用户制定培训与考核制度,确保他们能够充分理解和使用分析类技术,保证智能系统安全分析的准确性。

4) 应用类技术。应用类技术包括人工智能、区块链、大数据等,将人-机-环-管子系统串联起来,打破智能系统各子系统间的信息壁垒,通过技术赋能提高智能系统安全管理和应急响应能力。

分析应用类技术时,应重点关注人机交互的安全性、自动化与控制系统的安全性、应用程序的潜在漏洞以及数据泄露和隐私风险。定期检查应用功能,并提供开发支持,确保功能能够按照需求实现,并符合用户的使用习惯。通过定期评估和反馈,持续优化应用类技术的实施效果,确保系统具有良好的扩展性,能够应对未来多变的安全需求。

通过对感知、传输、分析和应用类技术的全面安全分析,可以识别并缓解智能系统可能面临的安全威胁,确保系统在不同操作环境中能够安全、可靠安全地运行。这种分析不仅有助于预防潜在的安全事件,还能为系统设计提供有力的安全保障。

3 智能系统信息全过程动态平衡分析

3.1 智能系统信息传输分析

5G 时代,智能系统依靠信息流动来维持其动态平衡,因此在安全分析时,必须充分考虑信息流动的稳定性和可靠性。信息在智能系统内部持续循环和流动,确保系统在面对外界变化时能够迅速调整并恢复平衡,这是系统正常运作的基础。一旦信息流动受阻或遭到攻击,系统可能会失去平衡,进而引发安全风险。因此,保障信息在传输过程中的安全性至关重要。

系统安全的维护依赖于对信息流动的有效监控和保护。在这个过程中,智能系统面临着各种安全风险,如数据泄露、篡改和未经授权的访问等。这些风险可能会导致系统做出错误决策,从而触发安全事故。因此,确保数据在各个传输环节中都能得到一致和全面的安全防护,是维持智能系统整体安全性和稳定性的必要条件。

在事故演变过程中,信息需要经历需求识别、产生、传递、处理等过程。香农通信模型将这一过程概述为真信源—信源—信道—信宿信息流动模型[31]。结合负系统特性,可以进一步分析智能系统中的信息传输过程,如图 6 所示。

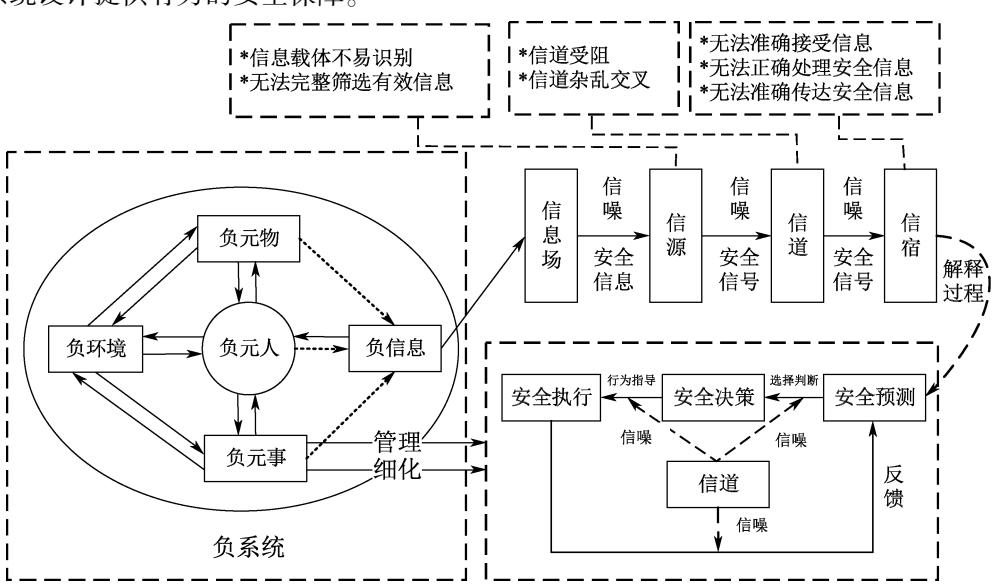

图 6 智能系统信息传输

Fig. 6 Intelligent system information transmission

由图 6 可知:智能系统中的信息流动往往是动态的,随着系统内人、事、物和外部环境的变化而不断调整。智能系统通过利用高新技术对系统中流转的安全信息进行分析处理,能够有效预测潜在的安全风险,并制定相关决策,为安全执行提供行为指导。因此,确保信息通过真信源—信源—信道—信宿的正确稳定传输是保证智能系统稳定动态运行的关键所在[32]。

笔者从负系统学思维范式出发,在智能系统信

息传输分析过程中,重点关注可能出现的负面情况,特别是那些可能破坏智能系统信息传输过程的因素,如信息失效、信息失真、通信不畅等问题。针对这些问题,应进行深入归类与分析。此外,还需重视在常态下智能系统信息处理的可行性与响应能力、信息传输过程中的循环反馈安全性、以及信息的冗余度和容错性等,以降低事故对系统安全的影响。通过全面的分析和防范措施,能够有效提升智能系统在复杂环境下的安全稳定性。

3.2　智能系统信息动态平衡分析

根据智能系统的开放包容性,系统具有能够与环境进行人、事、物、信息、能量等元素交换的能力和属性[17]。安全事故未发生时,智能系统中各元素、能量、伴随信息流动处于一种微妙的平衡状态,如图 7 所示。

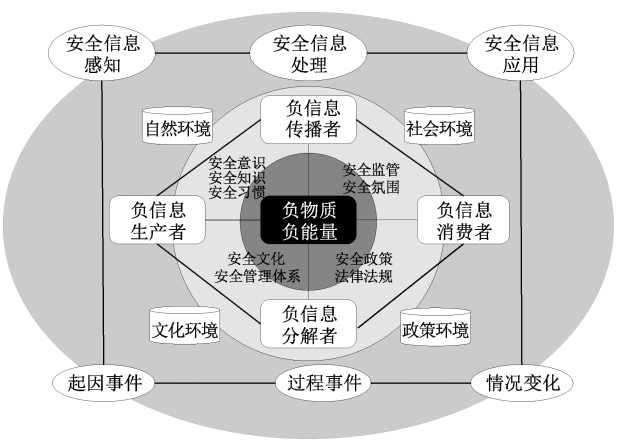

图 7　智能系统信息流动态平衡

Fig. 7　Dynamic balance of information flow in intelligent systems

在智能系统中,安全信息随着物质和能量的传递而流动,其感知、处理及应用过程与事故的起因、发展、变化同步进行。笔者将智能系统中的安全信息主体划分为生产者、传播者、消费者和分解者 4 种角色。信息作为载体在信息主体与周围环境之间循环流转,受内外环境的影响,同时也会间接影响环境,从而实现信息的产生、传递、循环、创新、修正和再生的动态平衡。

因此,在对智能系统进行安全分析时,不仅需要关注智能系统本身的技术构成和运行机制,还必须深入分析智能系统所处的广泛环境。这些环境包括自然环境、社会环境、政策环境以及文化环境等多方面的因素。自然环境涉及到智能系统与物理世界的互动,例如:气候变化、地理位置、自然灾害等都可能对系统安全产生影响;社会环境则涵盖了人类社会的复杂关系和行为模式,这些因素可能通过用户行为、社会结构、舆论导向等途径影响智能系统的安全性。同时,政策环境也是不可忽视的一个因素,不同的政策法规、行业标准和监管要求会对智能系统的设计和运行施加约束,从而影响其安全性。此外,文化环境亦扮演着重要角色,文化差异、价值观念和社会信仰等文化因素,都可能在智能系统的使用和接受过程中引发安全隐患。

除此之外,还应对信息主体的个体特性和组织内部的人文环境进行详细剖析。个体特性涵盖了用户的知识水平、操作习惯、心理状态等,这些因素直接关系到智能系统的使用方式和安全风险。而组织的人文环境则包括企业文化、管理模式、团队合作等方面,它们在智能系统的开发、部署和维护过程中可能产生潜在的安全威胁。因此,全面、综合地分析这些因素,是确保智能系统安全的重要前提。

3.3　智能系统信息全过程循环分析体系

基于负系统理论进行智能系统安全分析,重点关注系统中的负元素,观测其是否达到阈值。其中安全信息在系统中循环流动,作为逻辑主线带动智能系统运行。根据智能系统中信息的流动方向,对智能系统安全进行动态分析,具体分析如图 8 所示。

1) 对智能系统进行全谱系扫描。对智能系统内的人、物、事、信息进行信息提取,检验其是否达到系统阈值,是否实现负涌现,并将采集的信息上传至多维数据库储存。

2) 利用高新技术进行数据库信息采集。并对采集的信息进行归一化处理,以便进行后续的数据信息融合,然后将融合信息生成信号,信号经多重清洗、过滤,以提取智能系统安全分析所需信息。

3) 智能系统的安全态势风险感知与识别。将所提取的信息,按照觉察要素、理解要素、预测要素分类,通过对 3 类要素的分析,识别系统所涉及的危险情境[33]。

4) 风险评估与预测。通过数学统计学的方法,将识别到的风险、情境等用来评估智能系统安全事故的发生概率,致损能力和严重度等。利用相关数据,进行风险类别的预测、事故强度变化预测、风险的时间预测等。根据预测结果提醒组织成员进行预处理,从根本上降低事故损害程度。

5) 情景分析。通过建立重要性、不确定性联合表,将智能系统中的不确定性因素、重要性因素按规律排列,据此进行情景构建。利用仿真模拟软件,对事故情景进行仿真模拟,以此推断出智能应对方案。

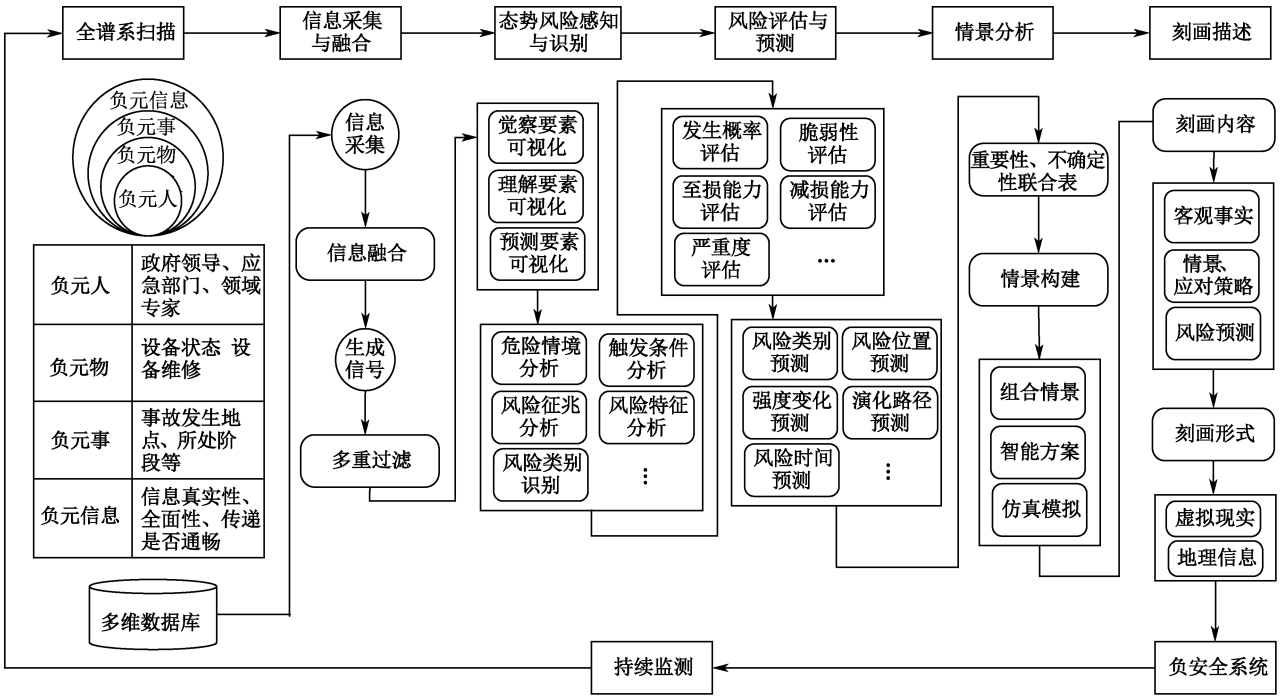

图 8　智能系统全过程安全分析体系

Fig. 8　Safety analysis framework for the whole process of intelligent system

6）刻画描述。将评估内容、预测内容、仿真结果进行内容刻画，结合客观事实，刻画出相应的事故情景，从而生成应对策略、预测结果。结果以虚拟现实和地理区域信息结果的形式显示，最后将数据上传至智能系统，并持续对相关数据进行事实检测，形成安全系统分析闭环。

4　结　论

1）根据智能系统的安全负系统表达与生物学意义上的生态系统的相似性，提出安全稳定的智能系统须具有开放包容性、交互耦合性、动态平衡性3个特性。

2）文中建立的5G时代负系统学视域下智能系统安全分析框架体系，能够有效分析智能系统的安全稳定运行及信息流动全过程的动态平衡，确保智能系统安全分析的全面性和可靠性。

3）未来研究可加入实证分析内容，推进智能系统安全分析流程的落地；另外，可继续拓宽研究视角，利用跨学科、跨领域理念与安全科学继续迸发出新的火花。

参 考 文 献

[1]　冯亚娟，邢仲超. 安全激励对安全创新行为的影响研究：知识共享和安全氛围的作用[J]. 软科学，2022，36(4)：110-117.
FENG Yajuan，XING Zhongchao. The impact of safety incentive on safety innovation behavior：the roles of knowledge sharing and safety climate [J]. Soft Science，2022，36(4)：110-117.

[2]　王慧军，安亮，高宇龙，等. 风险预控管理体系融合 ISRS 研究[J]. 中国安全科学学报，2021，31(增 1)：68-72.
WANG Huijun，AN Liang，GAO Yulong，et al. Research on safety risk pre-control management system and ISRS[J]. China Safety Science Journal，2021，31(S1)：68-72.

[3]　谢科范，梁本部，刘嘉，等. 安全 4.0 时代的安全生产管理模式研究[J]. 中国安全科学学报，2023，33(3)：19-26.
XIE Kefan，LIANG Benbu，LIU Jia，et al. Work safety management mode in Safety 4.0 era[J]. China Safety Science Journal，2023，33(3)：19-26.

[4]　AVEN T. What is safety science? [J]. Safety Science，2014，67：15-20.

[5] 吴超. 安全科学学的初步研究[J]. 中国安全科学学报, 2007,17(11): 5-15.
WU Chao. Initial study of the science of safety science[J]. China Safety Science Journal, 2007,17(11): 5-15.
[6] 张会平,赵溱,马太平,等. 我国数据要素市场化流通的两种模式与生态系统构建[J]. 信息资源管理学报, 2023, 13(6):29-42.
ZHANG Huiping, ZHAO Qin, MA Taiping, et al. Two modes and ecological system construction of data element market circulation in China [J]. Journal of Information Resource Management, 2023,13(6):29-42.
[7] 尹佳音. 美、日、印构建信息安全体系的思路与借鉴[J]. 宏观经济管理, 2021(4):84-90.
[8] 牛莉霞,李肖萌. 5G 时代智慧矿山安全管理新模式[J]. 中国安全科学学报, 2021,31(6):29-36.
NIU Lixia,LI Xiaomeng. A new safety management model of Intelligent Mines in 5G Era[J]. China Safety Science Journal, 2021,31(6):29-36.
[9] 褚健. 工业互联网时代工厂安全生产的思考与实践[J]. 科技导报, 2019,37(12):92-96.
CHU Jian. Plant safety production in industrial internet era[J]. Science & Technology Review, 2019,37(12):92-96.
[10] 房明,张毅,谭玥. 多因素耦合失效模式下地铁施工安全系统与管理模型[J]. 中国安全科学学报, 2024,34(5): 82-90.
FANG Ming, ZHANG Yi, TAN Yue. Safety system and management model of subway construction under multi-factor coupling failure mode[J]. China Safety Science Journal, 2024,34(5):82-90.
[11] 张充,张伟,李泽亚,等. 基于 SI-SB 系统安全模型的多层级边缘智能管控模式[J]. 中国安全科学学报,2024, 34(1):17-26.
ZHANG Chong, ZHANG Wei, LI Zeya, et al. Study on multi-level edge intelligent management and control mode based on SI-SB system safety model[J]. China Safety Science Journal, 2024,34(1):17-26.
[12] 张伟,廖阳新,蒋灵,等. 基于物联网的塔式起重机安全监控系统[J]. 中国安全科学学报,2021,31(2):55-62.
ZHANG Wei, LIAO Yangxin, JIANG Ling, et al. Safety monitoring system of tower crane based on internet of things[J]. China Safety Science Journal, 2021,31(2):55-62.
[13] 孙殿阁. 基于数字孪生技术的民用机场安全管理系统构建[J]. 中国安全科学学报, 2023,33(S1):222-227.
SUN Dian´ge. Research on the construction of civil airport safety management system based on digital twin technology[J]. China Safety Science Journal, 2023,33(S1):222-227.
[14] 杨帅. 工业 4.0 与工业互联网:比较、启示与应对策略[J]. 当代财经, 2015(8): 99-107.
[15] 化柏林,郑彦宁. 情报转化理论(下):从信息到情报的转化[J]. 情报理论与实践, 2012, 35(4): 7-10.
HUA Bolin, ZHENG Yanning. The theory of information transformation(Ⅱ): transformation from data into information[J]. Information Studies: Theory & Application, 2012,35(4):7-10.
[16] 化柏林,郑彦宁. 情报转化理论(上):从数据到信息的转化[J]. 情报理论与实践, 2012, 35(3): 1-4.
HUA Bolin, ZHENG Yanning. The theory of information transformation(Ⅰ): transformation from data into information[J]. Information Studies: Theory & Application, 2012,35(3):1-4.
[17] 吴超. 负系统学的创建研究[J]. 中国安全科学学报, 2023,33(3):1-10.
WU Chao. Negative systematology construction research [J]. China Safety Science Journal, 2023,33(3):1-10.
[18] 黄浪,吴超,王秉. 安全系学学科理论体系构建研究[J]. 中国安全科学学报, 2018,28(5): 30-36.
HUANG Lang, WU Chao, WANG Bing. Research on construction of safety systematics outline [J]. China Safety Science Journal, 2018,28(5):30-36.
[19] 吴超. 一组表达安全创新的新概念及其关联问题[J]. 安全, 2020,41(2):65-72.
WU Chao. A group of new concepts for showing safety innovation and their relevant problems[J]. Safety & Security, 2020,41(2):65-72.
[20] ARTHUR G T. The use and abuse of vegetational concepts and terms[J]. Ecology, 1935,16(3):284-307.
[21] 张夏恒,肖林. 元宇宙跨境电商信息生态系统:模型构建与治理思路[J]. 电子政务, 2023(3):85-94.
[22] 李炳军,曹斌,周方. 创新生态系统共生、绿色技术创新与低碳经济高质量发展[J]. 统计与决策, 2023,39(16): 48-53.
LI Bingjun, CAO Bin, ZHOU Fang. Innovation ecosystem symbiosis, green technology innovation and high-quality development of low-carbon economy[J]. Statistics & Decision, 2023,39(16):48-53.
[23] HADDON W. Energy damage and the ten countermeasure strategies[J]. SAGE Publications, 1973,15(4): 355-366.

[24] 黄浪,吴超,马剑. 安全信息流视域下的事故致因模型构建[J]. 管理评论, 2020,32(4):274-285.
HUANG Lang, WU Chao, MA Jian. An accident-causing model under the perspective of safety information flow [J]. Management Review, 2020,32(4):274-285.

[25] 雷长群. 安全生产领域基本概念辨析及双重预防机制研究[J]. 中国安全生产科学技术, 2017,13(2):17-21.
LEI Changqun. Study on basic concepts discrimination and double prevention mechanism in the field of work safety [J]. Journal of Safety Science and Technology, 2017,13(2):17-21.

[26] 傅贵,吴亚丽,章仕杰,等. 危险源的实质内容分析[J]. 中国安全科学学报, 2020,30(11):1-5.
FU Gui, WU Yali, ZHANG Shijie, et al. Analysis on essential content of hazard [J]. China Safety Science Journal, 2020,30(11):1-5.

[27] VESPIGNANI A. Predicting the behavior of techno-social systems[J]. Science, 2009,325(5939):425-428.

[28] 杜英,李晓玲,张爱宁. 内聚耦合视角下的产学研合作研究:以甘肃重大科技专项为例[J]. 中国科技论坛, 2016(4):43-48.
DU Ying, LI Huanling, ZHANG Aining. On the industry-university-research institute collaboration from the perspective of cohesion and coupling: a case study of gansu province major science and technology projects[J]. Forum on Science and Technology in China, 2016(4):43-48.

[29] 于兴尚,刘月,谭洪,等. 数智驱动下智慧图书馆的场景应用与模型体系建构[J]. 图书与情报, 2023(2):95-102.
YU Xingshang, LIU Yue, TAN Hong, et al. Scenario application and model system construction of smart libraries driven by digital intelligence[J]. Library & Information, 2023(2):95-102.

[30] 陈美华,仝鹏,李静,等. 数智化时代下情报赋能智慧应急的场景化应用研究:以元宇宙的应用开发为例[J]. 情报理论与实践, 2024,47(2):132-138,123.
CHEN Meihua, TONG Peng, LI Jing, et al. Scenario-based application of information empowering smart emergency in the age of digital intelligence: taking the application development of the metaverse as an example [J]. Information Theory & Practice, 2024,47(2):132-138,123.

[31] 吴超. 安全信息认知通用模型构建及其启示[J]. 中国安全生产科学技术, 2017,13(3):5-11.
WU Chao. Construction of universal model on safety information cognition and its enlightenment [J]. Journal of Safety Science and Technology, 2017,13(3):5-11.

[32] 李思贤,吴超,王秉. 多级安全信息不对称所致事故模式研究[J]. 中国安全科学学报, 2017,27(7): 18-23.
LI Sixian, WU Chao, WANG Bing. Study on model for accident resulting from multilevel safety information asymmetry [J]. China Safety Science Journal, 2017,27(7):18-23.

[33] 牛莉霞,李肖萌. 5G 时代面向情报需求的智慧矿山应急管理新模式研究[J]. 灾害学, 2024,39(3): 228-234.
NIU Lixia, LI Xiaomeng. Research on the new model of intelligent mine emergency management oriented to intelligence needs in the 5G era[J]. Journal of Catastrophology, 2024,39 (3):228-234.

作者简介: 牛莉霞 (1983—),女,山西吕梁人,博士,教授,主要从事组织行为管理与人因工程方面的研究。E-mail:327334231@ qq. com。

李肖萌 (1996—),女,河北秦皇岛人,博士研究生,研究方向为安全管理与安全心理学。E-mail:183475870@ qq. com。