DOI 10.15302/J-SSCAE-2025.08.038

韧性系统工程：概念、方法与挑战

杨林[1*]，王强[2]，匡洪宇[1]，操礼春[1]，马小山[1]，李峰[1]，任保全[1]

（1. 军事科学院系统工程研究院，北京 100091；2. 军事科学院军事智能研究院，北京 100091）

摘要：智能时代的复杂系统具有多域互联、“人–机–物”高度融合等特征，在开放、动态甚至对抗环境下受到多维扰动威胁，生存性、可用性面临挑战。针对经典系统工程理论方法在应对不确定性、突发扰动方面的不足，本文提出了韧性系统工程概念并构建了方法框架，探索了系统设计阶段的“韧性设计内置”，以提升复杂系统持续运行与适应演进能力。梳理了韧性概念的多学科定义与内涵，明确了扰动因素分类、韧性能力阶段划分，对比了韧性与容错性、生存性、安全性、鲁棒性等的差异性。在经典系统工程理论方法的基础上引入了韧性理论要素，提出了韧性系统工程的概念与方法流程，将预防、抵御、适应、恢复、演进等韧性能力融入系统全生命周期设计中。构建了涵盖通用指标、领域特定指标，由定量评估、定性评估构成的韧性度量框架，并以自主巡航机器人系统为例阐述了韧性系统工程方法的应用过程。以电力能源系统、信息通信网络、无人智能系统、供应链网络为典型领域，探讨了韧性理论方法的工程化探索情况，进而辨析了落地应用面临的挑战。通过持续的理论创新、方法完善、工程实践，将韧性系统工程发展成为系统工程的新范式，为关键基础设施、智能无人装备、复杂系统的安全可靠与持续运行提供坚实的理论方法支撑。

关键词：韧性；系统工程；韧性系统工程；韧性评估；基于模型的系统设计；形式化方法

中图分类号：N945　　**文献标识码：**A

Resilience Systems Engineering: Concepts, Methods and Challenges

Yang Lin[1*], Wang Qiang[2], Kuang Hongyu[1], Cao Lichun[1], Ma Xiaoshan[1], Li Feng[1], Ren Baoquan[1]

(1. Systems Engineering Research Institute, Academy of Military Sciences, Beijing 100091, China; 2. Military Intelligence Research Institute, Academy of Military Sciences, Beijing 100091, China)

Abstract: Complex systems in the intelligent era are characterized by multi-domain interconnection and deep integration of human, machine, and things. Operating in open, dynamic, and even adversarial environments, these systems are exposed to multi-dimensional disturbance threats, posing severe challenges to their survivability and usability. To address the limitations of classical systems engineering theories and methods in handling uncertainties and sudden disturbances, this study proposes a concept of resilience systems engineering and constructs its methodological framework. It explores the paradigm of “built-in resilience design” during the system design phase, aiming to enhance the continuous operation, adaptive, and evolutionary capabilities of complex systems. Moreover, the study sorts out the multidisciplinary definitions of resilience, clarifies the classification of disturbance factors and the division of resilience capability phases, and compares the differences between resilience and other related concepts such as fault tolerance, survivability, security, and robustness. On the basis of classical systems engineering theories and methods, this study

收稿日期：2025-08-24；**修回日期：**2025-12-12

通讯作者：*杨林，军事科学院系统工程研究院研究员，研究方向为网络安全与系统工程；E-mail: yanglin61s@sina.com

资助项目：基础加强计划重点项目(2025-JCJQ-ZD-015-00)；某综合研究项目(JK2023B010300-4)

本刊网址：sscae.engineering.org.cn

introduces the theoretical elements of resilience, proposes the concept and methodological process of resilience systems engineering, and integrates resilience capabilities (including prevention, resistance, adaptation, recovery, and evolution) into the full lifecycle design of systems. A resilience measurement framework is established, which covers both general indicators and domain-specific indicators, and consists of quantitative and qualitative evaluation dimensions. Taking the autonomous cruise robot system as a case study, the study elaborates on the application process of the resilience systems engineering method. Focusing on typical fields including power energy systems, information and communication networks, unmanned intelligent systems, and supply chain networks, this study discusses the engineering exploration of resilience theories and methods, and further analyzes the challenges faced in their practical implementation. Through continuous theoretical innovation, methodological improvement, and engineering practices, resilience systems engineering is expected to evolve into a new paradigm of systems engineering, providing solid theoretical and methodological support for the safe, reliable, and continuous operation of critical infrastructure, intelligent unmanned equipment, and complex systems.

Keywords: resilience; systems engineering; resilience systems engineering; resilience assessment; model-based system design; formal methods

一、前言

随着信息通信、人工智能（AI）等技术的发展，复杂系统在“人–机–物”深度融合的背景下呈现高度互联、跨域耦合等特征[1]，在拓展系统功能边界和运行能力的同时，加剧了系统的脆弱性和不确定性风险。复杂系统通常部署在高度不确定、动态变化甚至存在恶意对抗的环境中，面临从软硬件故障、物理损伤、环境突变到网络攻击、电磁干扰、认知欺骗的多维度、多域（物理 / 电磁 / 信息 / 认知）复合威胁。从日本福岛核事故到美国得克萨斯州电网瘫痪，再到局部冲突中供应链脆弱性、AI 系统误判事件，都揭示出在关键基础设施、国防军事等领域中复杂系统在面临扰动时存在功能失效、级联失效等风险。因此，在动态、多变甚至对抗性的环境下，确保系统能够持续提供核心功能服务并完成使命任务，成为学术界与工程界亟待应对的核心问题。

韧性作为系统在不利条件下维持、恢复并演进其核心功能的能力[2,3]，是应对上述挑战的重要概念，也成为复杂系统设计与运行维护的关键属性。从发展历程看，韧性概念最初用于描述物质在形变后恢复原状的能力[4]。1973 年，有学者将韧性引入生态学范畴并提出了生态韧性概念，即生态系统在维持基本功能的前提下吸收扰动并适应变化的能力[5]，由此拓展了韧性的内涵并使之从物理恢复能力向系统适应性转变。2007 年，国际系统工程协会（INCOSE）成立了韧性系统研究专业组，面向复杂系统的脆弱性问题，聚焦韧性系统的实践方法与技术工具等标准化研究[6]。2011 年，美国 MITRE 公司发布了首部《赛博韧性工程框架》[7]，界定了赛博韧性的理论内涵与工程实现路径[8]。2018 年，荷兰理工大学联盟成立了韧性工程研究中心，致力于提升“社会–技术–环境”复杂系统的综合韧性。2019 年，美国国家标准与技术研究院颁布《开发赛博韧性系统：系统安全工程方法》，确立了韧性系统工程化实施框架[9]。2022 年，欧盟发布《赛博韧性法案》，将韧性要求纳入法规体系[10]。自 2023 年起，韧性系统国际会议持续聚焦供应链、基础设施、AI、数字系统、灾害管理、能源等领域的议题，将韧性确定为系统工程研究的重要前沿。然而，当前研究集中在特定领域的韧性机理层面，缺乏从系统工程方法论角度出发的统一理论与实践框架，尚不能全面支撑复杂任务关键系统的“韧性设计内置”。

系统工程作为解决复杂系统研制与管理问题的经典理论及方法体系，定义并规范了系统研制过程中包括需求分析、架构设计、验证确认在内的全生命周期设计与管理等工程活动，在航空航天、电力网络等典型领域开展了长期应用实践，形成了较为成熟的理论与实践体系[11]。系统工程的主要关注点是应对系统复杂性，确保在成本、进度可控的情况下实现系统整体功能、性能的最优，在一定程度上能够解决大规模系统集成、跨学科协同、生命周期管理等方面的问题。然而，经典的系统工程主要建立在系统需求相对确定、运行边界可控的前提假设之上，对于高度不确定、智能演化甚至对抗条件下的复杂系统仍存在诸多不足，突出表现在缺乏应对扰动和对抗等不确定性因素的动态响应机制、韧性能力未能在生命周期的早期阶段实现设计内置、未考虑系统的自适应与演进能力。这些局限成为引入韧性理论的重要原因，也构成韧性系统工程发展的逻辑起点。

本文在经典系统工程理论方法体系的基础上引入韧性理论要素，提出韧性系统工程的概念与方法，以确保系统在动态、多变甚至对抗性的环境下具备持续提供核心功能服务并完成使命任务的能力。具体地，从系统工程的视角出发，界定并辨析韧性的概念与内涵，明确韧性与可靠性、容错性、生存性等相关概念的关系；建立韧性系统工程的方法流程，将预防、抵御、适应、恢复、演进的阶段性能力设计贯穿系统全生命周期，推进“韧性设计内置”；初步构建韧性评估指标与度量框架，推动韧性从抽象理念转化为可建模、可验证的工程实践。

二、韧性与韧性系统工程

（一）韧性的概念与内涵

系统趋于复杂与高度互联，在面对各类扰动时显现出脆弱性。与之相关的网络安全、容错计算、可靠性工程、网络生存性等领域分别从不同视角开展了韧性研究，反映了工程实践中系统对应对扰动能力的迫切需求，推动了韧性理论从单一维度向多学科融合的演进。鉴于系统类型多样性、应用场景差异性、研究视角多元化，学术界与工程界对韧性的定义尚未形成共识。为了构建韧性系统工程的理论与方法体系，需要从工程实践的视角对韧性的核心内涵进行清晰的界定。

1. 韧性的概念

目前，系统韧性[12~20]、体系韧性[21]、赛博韧性[22~28]、网络韧性[29~32]、协作韧性[33]等是工程领域中的主要研究方向（见表1）。系统韧性强调系统在扰动发生前后展现的动态响应与恢复能力，包含对稳定性的维持、对性能退化风险的容忍，目标是保障系统在不利条件下仍能实现核心功能的连续性与任务的完整性。当系统复杂度上升至由多个相对独

表1　相关领域韧性定义概述

领域	定义	文献
系统韧性	系统或组织在早期阶段对干扰做出反应并从中恢复，以最小化对系统性能动态稳定性影响的能力	[12]
	系统从干扰中恢复到受干扰前的某种性能水平的能力	[13]
	复杂系统对干扰的预防、吸收、适应、恢复能力	[14]
	安全漏洞可被检测、遏制并获得解决的能力	[15]
	系统在面对变化时能够持续、可靠满足需求的能力	[16]
	系统遭遇变化时保持可靠性和安全性，可承受损害或从中恢复的特性	[17]
	系统在不利条件下实现能力交付的一种体现	[18]
	系统在压力条件下以降低服务质量来维护核心功能运行的特性	[19]
	在持续的对抗性环境下，系统的核心关键功能仍保持正常运行，确保受影响功能可在预定义成本限制内得到恢复	[20]
体系韧性	在不同的恢复策略下体系的性能恢复能力	[21]
赛博韧性	在面临变化时仍能合理可信地持续提供服务的能力	[22]
	为应对潜在的不利事件而进行的准备和规划、吸收不利事件影响，从中恢复或更好适应的能力	[23]
	系统在遭受网络攻击导致性能下降后恢复或再生系统性能的能力	[24]
	系统在变化过程中以及变化发生后能够自我稳定状态的能力	[25]
	系统、组织、任务、业务流程对运行所需网络资源面临的对抗性条件、压力、攻击的预见、承受、恢复、适应能力	[26]
	系统或服务在遭受攻击后通过快速自动化回滚并恢复正常运行的能力	[27]
	系统对不利影响进行准备、承受、恢复、适应的能力	[28]
网络韧性	网络面对各种故障和挑战时提供并维持可接受服务水平的能力	[29]
	网络化系统保留基本功能的能力	[30]
	网络在面对故障和挑战时提供并维持可接受服务水平的能力	[31]
	网络在某种故障模式（随机或人为）下承受性能下降、在受损节点数量增加的情况下继续传递消息的能力	[32]
协作韧性	群体系统在面临威胁或破坏性事件时具备预见、准备、抵御、恢复、实现转变的能力	[33]

立子系统构成的体系时，传统的单体恢复机制将难以满足整体系统的韧性需求。为此，韧性设计需从局部能力拓展至整体适应性层面，即上升至体系韧性。赛博韧性、网络韧性作为系统韧性的特定应用形态，分别聚焦信息系统、网络结构在面对攻击、故障、异常状态时的恢复与适应能力。协作韧性是智能时代韧性研究的新方向，强调在智能集群系统中多个自主实体通过分布式信息共享、行为自主协调、策略智能协同来提升系统在不利条件下的适应性与演进能力。

在工程系统领域，通常根据具体的应用场景和关注重点而从不同侧面对韧性进行描述。本研究结合长期工程应用实践以及对工程领域韧性的理解，将韧性定义为：系统在不利条件下完成使命任务并适应演进的能力。由此明确了韧性研究的终极目标是使命任务的达成，将适应演进作为高阶能力以为系统工程活动提供清晰的导向。

2. 韧性的内涵

本研究认为，有别于传统属性对系统局部或静态特征的关注，韧性是系统为完成核心使命而在全生命周期内应对扰动的一种动态且主动的能力。具有韧性的系统，价值不仅体现在功能性可满足预期的需求，而且能够在不利条件下快速重构、适应环境变化并持续演化以最终完成使命任务。以军用网络系统为例，当特定通信节点因遭受攻击而瘫痪时，系统能够通过备用通道自动重新路由通信，确保节点之间信息流的连续性，从而完成关键信息传输任务。韧性的核心内涵在于，当面临不利条件的扰动时，采用差异化的能力阶段实现机制，确保容错性、可靠性、鲁棒性、生存性、安全性等，最终达到任务要求（见图1）。

（1）扰动因素

识别潜在的扰动因素是设计韧性系统的基本前提，也是韧性系统工程方法中“不利条件分析”阶段的直接输入。扰动可解构为3个层级：缺陷（系统的潜在瑕疵），错误（缺陷触发导致系统状态异常），失效（系统行为偏离预期目标）[34]。本研究据此提出广义扰动概念，将扰动定义为所有可能对系统功能、性能、运行状态产生影响的因素，包括硬件故障、软件缺陷、人为攻击等传统扰动，系统升级、规模扩展等主动变更行为。例如，Kubernetes集群在写入数据时需要复制到多数节点以保证一致

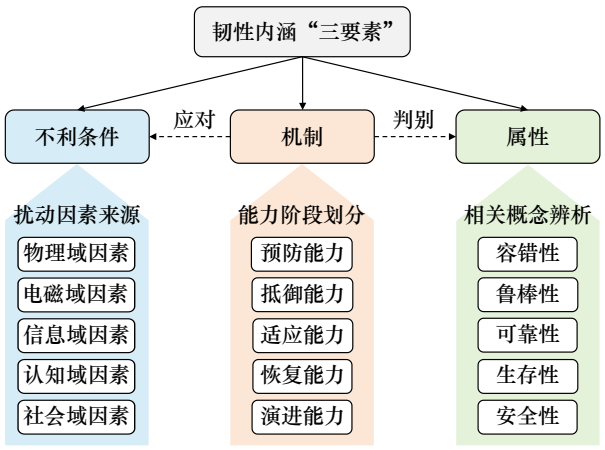


图1　韧性的概念内涵

性，这一机制虽然提高了可靠性，但是显著增加了写入延迟[35]，也带来了系统扰动。

涉及扰动来源的领域至少有物理域（如硬件故障、毁伤），电磁域（如干扰、压制），信息域（如漏洞、攻击），认知域（如欺骗、诱导），社会域（如人机交互故障、协同失效）。相关扰动还可进一步分类：在动机视角下，分为蓄意扰动（如网络攻击）、无意扰动（如兼容性故障）；在作用范围方面，分为内部扰动（如软件漏洞）、外部扰动（如电磁干扰）；在持续性方面，分为瞬态扰动（如短暂信号干扰）、永久性扰动（如硬件损毁）；在影响层级方面，分为局部干扰（如单节点失效）、系统性干扰（如级联故障）；在可预测性方面，分为可预见干扰（如季节性负载波动）、不可预见干扰（如零日漏洞攻击）。对扰动来源及类型进行分类，构成了韧性系统工程中进行风险识别、脆弱性分析、韧性机制设计的底层依据。

（2）能力阶段

系统功能、性能随时间的变化通常由韧性曲线刻画[36]。韧性曲线不仅是韧性评估的可视化工具，相应阶段划分更是对应着韧性系统工程方法中需要设计和嵌入的具体能力。从系统应对扰动发生、存续的时间维度，可将韧性能力划分为预防、抵御、适应、恢复、演进5个阶段（见图2）。① 预防阶段，为系统未受扰动的正常运行时期。应用风险预测、系统加固、冗余备份等策略，在扰动发生前主动降低系统的脆弱性，以最小化扰动发生的可能性与影响范围[29]。② 抵御阶段，为系统因遭受扰动开始出现能力退化现象的时期。应用故障隔离、负载

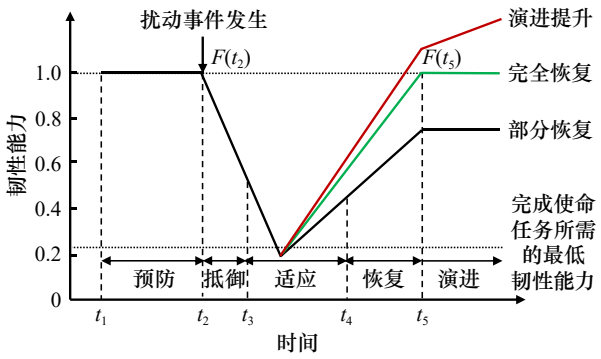


图2　韧性能力阶段示意图

注：t表示时间；F表示系统韧性能力随时间变化的函数；$F(t_2)$、$F(t_5)$表示初始能力水平，$[t_3,t_4]$表示任务允许的系统适应中断的最长时间。

均衡等策略对系统进行实时防护，以最大程度地抵御能力降级[12]。③ 适应阶段，为系统持续遭受扰动但仍能维持任务能力的时期。通过参数和行为调控来适应扰动的不利影响，以维持系统提供关键功能的能力[17]。④ 恢复阶段，为系统消除扰动的不利影响、逐步恢复业务功能并完成使命的时期。通过重配置、状态回滚、状态增强等技术手段，实现功能或性能的恢复。⑤ 演进阶段，为系统进入新稳态运行的时期。从扰动数据中学习经验，通过体系结构、流程、机理等方面的调整，使系统突破原始能力边界并演化形成新的能力基线。这5个阶段共同构成覆盖“事前–事中–事后”的完整能力闭环，以提升系统的预防、抵御、适应、恢复、演进能力为核心目标，来指导和贯穿下文韧性系统工程方法流程中“双V模型”各阶段的活动设计。

（3）相关概念辨析

韧性是系统应对多重扰动并完成核心使命的关键能力，相应内涵涉及并超越了容错性、生存性、安全性、鲁棒性等传统属性的范畴[12,14,37~39]。在多维度解构分析的基础上给出了韧性与其他系统属性的差异（见表2）。在目标维度，韧性以完成核心使命任务为最高目标，与仅关注功能层面稳定性的其他属性有区别。在响应维度，韧性贯穿扰动发生的全生命周期，形成“预防–抵御–适应–恢复–演进”完整闭环。在时间维度，韧性体现为“即时响应–短期恢复–长期演进”的递进式能力链。在价值维度，韧性实现从功能维持到使命保障再到能力演进的价值跃迁。整体上，韧性具有多维特性，成为安全、可靠、鲁棒等属性的集中体现。

（二）韧性系统工程的定义

在系统工程的理论体系方面，文献[40]首次提出了系统工程方法论，被视为系统工程的奠基之作；软系统方法论[41]强调在复杂不确定环境中的系统思维，为应对系统工程中的模糊性与对抗性问题提供了关键支撑；进一步发展的系统工程完整理论框架[42]，强调系统思维和全生命周期管理，契合系统工程的技术性、管理性双重属性；也有观点认为，系统工程是将功能、性能、成本、进度进行一体化设计的集成方法[43]。在行业标准方面，国际系统工程协会发布手册文件[11]，确立了系统工程的通用标准，定义了基于模型的系统工程以及SysML 2.0和跨域协同建模实践。近年来，基于模型的系统工程成为重要研究方向，如探讨了基于模型的系统工程的现状和趋势[44]，将系统工程拓展到社会–技术系统，采用侧重跨学科方法应对系统性和不确定性风险[45]。

自20世纪50年代起，钱学森开创并引领了我

表2　韧性相关概念的特征对比

相关概念	核心目标	典型扰动	关键能力
韧性	在不利条件下也能够完成使命任务	自然灾害、网络攻击、电磁干扰、认知欺骗	预防、抵御、适应、恢复、演进
容错性	在已知/预期故障下维持预设核心功能	内部故障、预期错误	冗余、隔离、故障处理
生存性	遭受毁灭性打击后维持最基本关键功能	极端事件、毁灭性攻击/灾害	最小核心保护、应急操作
鲁棒性	在参数变化/输入扰动下保持稳定运行	非致命干扰、不确定性、噪声	稳定性、抗干扰
可靠性	在规定条件/时间内无故障运行	内部故障、组件失效	故障预防、高可用性
安全性（Safety）	避免对人员/环境/财产造成不可接受伤害	非恶意物理风险、操作失误	风险评估、危害控制、失效安全
安全性（Security）	保护系统免受恶意攻击，确保机密性、完整性、可用性及其他安全属性	物理入侵、网络攻击、社会工程	预防、检测、响应、取证

国系统工程事业，提出了系统工程是组织和管理技术的观点，也强调系统工程具有与国家重大工程实践紧密结合的特征[46]；指出系统工程的精华是系统观点，系统工程是处理系统的工程技术[47]。在对钱学森系统工程理论思想发展过程进行考察分析的基础上，总结了系统工程的本质特征即为采用系统观点处理问题的工程技术[48]。受钱学森系统科学思想的启发提出了知识系统工程的概念，认为知识系统工程是对知识进行组织管理的技术[49]。针对学术界对系统工程的含义存在不同解读的情况，有研究认为系统工程是成功实现工程系统的方法和技术，应从需求出发并综合多种专业技术，支持开发整体性能优化的系统[50]。当前，系统工程在我国大型复杂技术项目中获得了广泛且深入的应用。例如，采用系统工程方法开展了风云三号卫星观测能力设计、地面系统顶层设计，统筹卫星和地面系统需求，最大化地面应用系统的整体能力[51]；对载人航天工程空间应用系统太空探索的方法和经验进行总结、梳理、凝练，形成了价值可持续太空探索的系统工程方法体系，确保太空探索活动在具有成果产出效益的条件下成本可承受、状态可保持[52]；在钱学森“可靠性之问”（如何将可靠性较低的元件组成可靠性较高的系统）的引导下，进一步发展了可靠性系统工程[53~56]，认为可靠性系统工程是研究产品全生命过程并同故障作“斗争”的工程技术。

系统工程在一定程度上支持解决了大规模系统集成、跨学科协同、生命周期管理等方面的重大问题，为韧性系统工程的构建提供了理论支撑。而客观上，对于高度不确定、智能演化、强博弈对抗条件下的复杂系统构造，系统工程仍存在诸多不足。这成为引入韧性理论的重要原因，也构成韧性系统工程发展的逻辑起点。需要将系统应对扰动等不确定性因素的能力视作与功能、性能同等重要的设计目标；也应将韧性能力覆盖至系统全生命周期，而不仅局限于设计或者运行某个特定阶段的基本特征；还应当以确保使命任务的可持续性为牵引，赋予系统长期的适应和演进能力。

韧性系统工程是以经典系统工程理论方法体系为基础，在系统性融入韧性理论要素后形成的系统工程新范式，相应定义为：实现系统在不利条件下完成使命任务并适应演进的系统工程方法。韧性系统工程作为一种跨学科、面向目标系统全生命周期的方法论，旨在运用系统工程基本理论，实现韧性系统的设计、验证、集成、部署、维护。韧性系统工程以实现系统的“内生韧性”或者“韧性设计内置”为目标，将韧性能力贯穿至包括系统设计、研制开发、部署运用在内的全生命周期活动中，将预防、抵御、适应、恢复、演进等阶段能力映射为具象且可建模的结构组件与控制策略，将冗余、可重构、故障隔离、优雅降级等韧性实现策略融入系统工程活动中，协同设计韧性机制与系统功能架构，使韧性成为系统的固有能力属性（而非额外的附加属性[57]）。

也要注意到，区别于传统系统工程对装备运行、服务连续的关注，韧性系统工程将高度不确定、对抗性环境下的多域级联扰动视为系统面临的固有不利因素，以完成使命任务作为牵引系统设计的主要目标；在强调功能、性能、成本、进度均衡的同时，通过韧性设计“左移”（而非事后评估、运行时补偿）实现在开放、动态、对抗环境中系统韧性能力的设计内置。此外，韧性系统工程以模型为载体，追求韧性在系统全生命周期中的可演化、可验证、可评估，调控预防、抵御、适应、恢复、演进等能力阶段，实现能力基线维持、效能恢复、能力演进。

三、韧性系统工程方法

韧性系统工程方法指实现系统韧性的系列工程方法，形成韧性系统工程协同设计、测试评估、验证确认的总体方法流程。主要分为系统韧性设计、系统韧性评估两个阶段，分别涉及韧性系统工程方法流程、系统韧性评估。

（一）韧性系统工程方法流程

韧性系统工程方法在系统工程“V”模型的基础上，以完成使命任务为牵引，将不利条件下预防、抵御、适应、恢复、演进等阶段能力的设计、评估、验证一体纳入系统工程的各阶段设计；在特定的资源和成本约束下，闭环全流程系统功能、性能、韧性协同设计与验证评估，形成“双V”模型，构建覆盖需求分析、架构设计、测试评估、验证确认的韧性系统工程设计方法，支持系统韧性的迭代演进（见图3）。

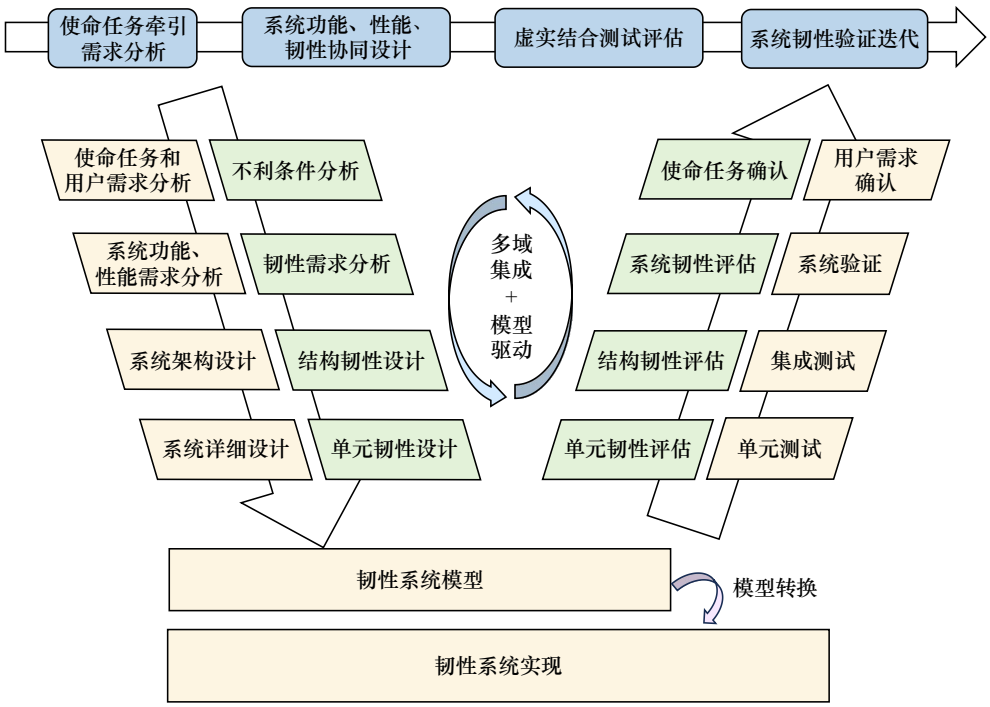


图3　韧性系统工程方法流程

在使命任务、用户需求分析阶段，进行系统可能面临的物理摧毁、电磁干扰、网络攻击等不利条件分析，解构对系统功能、性能的作用机理以及影响传播路径。在系统功能、性能需求分析阶段，基于不利条件研判结果，构建系统韧性需求模型，与系统功能、性能需求模型进行集成。在系统架构设计、详细设计阶段，以多域协同建模与集成的方式开展结构韧性（如功能解耦、冗余设计）和单元韧性（如组件自愈、局部容错）设计，将韧性能力嵌入系统的架构、行为、运行机制，构建韧性系统模型。在整个设计阶段，韧性不再是系统的运行态补偿，而是贯穿全流程的内在能力。在验证评估阶段，结合单元测试、集成试验、系统验证，基于数字模型驱动的多域集成、虚实结合仿真测试，从单元韧性、结构韧性、系统韧性的不同层次并由局部到整体地开展系统韧性能力的测试评估与验证，最终结合用户需求确认进行使命任务确认。

应用语义保持和韧性感知转换[58,59]，从韧性系统模型、运行平台模型、外部环境模型中推导并得出韧性系统的具体实现。模型转换过程主要包括韧性系统模型扩展、可执行代码生成：前者融合运行平台（硬件）模型（即软件组件到硬件单元的映射），构造扩展的韧性系统模型并用于设计空间遍历与优化[60]；后者通过设计模型与代码的映射及组合规则，自动生成面向特定平台的可执行代码。对韧性系统模型进行严格的形式化验证，证明基于模型的代码生成过程的正确性，确保在系统实现阶段落实设计阶段定义的预期韧性能力。

（二）系统韧性指标与度量方法

系统韧性度量作为韧性系统工程方法的重要组成，直接决定系统完成使命任务的韧性能力。通常采用定量评估、定性评估或两方面结合的方式度量系统韧性。其中，定量评估主要应用在韧性系统工程流程中的单元韧性、结构韧性、系统韧性评估阶段，定性评估主要应用在需求分析、使命任务确认阶段。

1. 韧性定量评估指标与方法

开展韧性定量评估，首先需明确用于衡量系统韧性的度量指标。本研究采用单调且连续函数进行韧性度量指标设计[61]。将系统韧性定量评估指标划分为通用评估指标、领域特定评估指标两类。通用评估指标基于韧性曲线进行设计[36,62~69]，常用的有4种。① 韧性损失速度，反映系统预防和抵御不利条件影响的能力。损失速度越小表示系统韧性越强，可通过计算韧性曲线在抵御阶段的斜率进行定

量评估（见图4中的橙色实线）。具体地，$F(t)$表征流量、延迟等物理量在不利条件下随时间的变化过程。若t_2为不利条件产生影响的时刻，则系统在$t(t_2 \leqslant t \leqslant t_3)$时刻的韧性损失速度可表示为$R(t)=\left(F(t_2)-F(t)\right)/(t-t_2)$。② 韧性损失量，刻画系统在不利条件作用过程中韧性随时间变化的累积效应，也反映系统预防和抵御不利条件影响的能力。损失量越小表示系统韧性越强，可通过计算韧性曲线在抵御阶段的面积积分或差值进行定量评估（如图4中的灰色阴影区域）。系统在$[t_2,t_3]$期间的韧性损失量可表示为$R(t)=\int_{t_2}^{\min(t,t_3)} F(t_2)-F(u)\mathrm{d}u$。③ 韧性恢复速度，反映系统适应不利因素的负面影响并恢复演进的能力。恢复速度越大表示系统韧性越强，可通过计算韧性曲线在恢复阶段的斜率进行定量评估（如图4中的红色实线）。若系统在t_5时间完成恢复，则系统在$t(t_4 \leq t \leq t_5)$时刻的韧性恢复速度可表示为$R(t)=\left(F(t)-F(t_4)\right)/(t-t_4)$。④ 韧性恢复量，数值越大表示系统韧性越强。与韧性损失量相对应，可通过计算韧性曲线在恢复阶段的面积积分或差值进行定量评估（如图4中的绿色阴影区域）。系统在$[t_4,t_5]$期间的韧性恢复量可表示为$R(t)=\int_{t_4}^{\min(t,t_5)} F(v)\mathrm{d}v-F(t_4)$。

上述指标物理含义清晰、计算方法简洁，结果具有可解释性，但主要用于表征单个阶段的韧性能力，难以全面刻画系统韧性的动态演化和全局性特征[70]。为此，定义1个综合的韧性评估指标[71]，将系统在不同能力阶段的韧性指标进行集成来构造统一的韧性评估指标函数（但未将不利因素考虑在内）：

$$GR=RL\times\left(RAPI_{RP}/RAPI_{DP}\right)\times\left(1/TAPL\right)\times RA \quad (1)$$

式（1）中，RL为系统的最低性能水平，$RAPI_{RP}$为性能恢复速度，$RAPI_{DP}$为性能下降速度，$TAPL$为性能损失量，RA为性能恢复量。此外，为了将系统的结构特征（如模块化设计、冗余设计）融入韧性评估过程，可从系统组成结构的角度出发，将系统功能、拓扑结构的冗余度指标应用到系统韧性的评估[72]；在一定程度上反映系统预防和抵御不利因素（如硬件故障）的能力，但依然无法准确衡量系统在不利条件下的适应、恢复、演进能力。

本研究在上述韧性评估指标的基础之上，将系统可能面临的不利条件引入定量指标构造，用于反映当前系统在开放动态环境中应对多种不利条件的韧性能力，由此形成韧性评估的三维空间（见图5）。在韧性能力随时间的二维空间变化轨迹的基础上，将同一使命任务时间窗口内系统面临的多个不利条件作为第三维度，综合考虑系统在多个不利条件下呈现预防、抵御、适应、恢复、演进等韧性能力变化的轨迹。鉴于各类不利条件的发生通常具有时间窗约束下的概率性、对韧性的影响权重具有差异性，假设不利条件之间互相独立，采用加权平均方式累计各个不利条件对韧性能力的影响。

考虑n种不利条件的影响，第i种不利条件事件发生概率为P_i，则评估系统韧性可采用下式：

$$\begin{aligned}R(t)=\sum_{i=1}^{n}P_i\times&\left(\int_{t_2}^{\min(t,t_3)}F_i(t_2)-F_i(u)\mathrm{d}u\right)^{-1}\times\\&\left[\int_{t_4}^{\min(t,t_5)}F_i(v)\mathrm{d}v-F_i(t_4)\right]\times\\&\left[\left(F_i(t_2)-F_i(t)\right)/(t-t_2)\right]^{-1}\times\\&\left[\left(F_i(t)-F_i(t_4)\right)/(t-t_4)\right]\end{aligned} \quad (2)$$

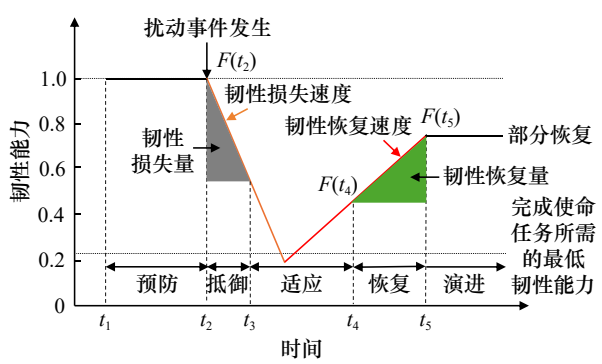


图4　通用韧性评估指标

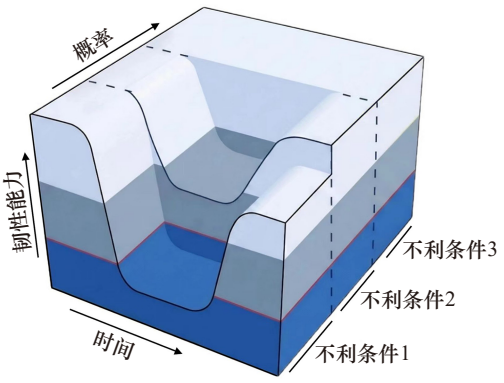


图5　结合不利条件的通用韧性评估指标示意图

式（2）中，$\int_{t_2}^{\min(t,t_3)} F_i(t_2)-F_i(u)\mathrm{d}u$表示系统在不利条件下韧性能力降级程度，$\int_{t_4}^{\min(t,t_5)} F_i(v)\mathrm{d}v-F_i(t_4)$为系统韧性能力恢复量，$(F_i(t_2)-F_i(t))/(t-t_2)$反映系统在不利条件下韧性能力降级的速度，$(F_i(t)-F_i(t_4))/(t-t_4)$反映系统从不利条件中韧性能力恢复的速度。

通用评估指标具有一般性的描述特征，适用于不同领域的系统韧性评估。在具体开展定量评估时，还需结合特定领域系统的使命任务、场景、结构等，对通用评估指标进行领域定制化设计。例如，通信网络领域通常选取基于服务质量的评估指标进行韧性评估，如量化数据传输的吞吐量、测量传输时间延迟、评估信号保真度的误码率、评价反映资源分配效率的带宽利用率等；电力系统领域常用的评估指标有停电频率、平均停电时长、特定时间内可恢复的负荷量等；交通领域的关键评估指标包括行程时间可靠性、交通拥堵恢复时间等。

2. 韧性定性评估方法

定性评估主要依赖实践经验、案例归纳等总结性分析，以逻辑描述的方式评估和分析韧性能力，如面向工程与系统测试的作战韧性框架中的韧性能力定性评估方法[73]。对于特定的系统，依赖领域专家对系统韧性进行评估，内容覆盖三方面：感知或发现不利条件（如网络攻击）的能力，识别系统中遭受不利条件影响的功能单元的能力，重新配置系统以适应不利条件的能力。赛博韧性矩阵[23]是另一个获得广泛应用的定性评估方法，定义了4×4韧性评估矩阵作为结构化定性评估的完整框架：综合审视物理、信息、认知、社会4个领域的赛博韧性，针对每个领域划分准备、吸收、恢复、适应4个阶段，再由专家进行能力评估。

3. 韧性评估方法的综合对比与应用场景

整体上，定量评估依赖数学模型、仿真工具、可量化的指标数据，适用于追求精确规范的业务场景。在AI技术快速发展的背景下，采用基于标注数据集和AI的方法进行韧性评估成为新动向，如基于深度学习的韧性推理框架无需依赖预定义的动力学模型或拓扑假设，可直接从观测数据中推断出系统韧性[74]。然而，不利条件的发生难以预知、训练和测试数据缺失，致使相关方法的实际使用场景受限。定性评估高度依赖领域专家的知识经验和认知水平，具有操作简单、主观性强的特点，适用于数据不足而难以量化或者对专家经验有较强依赖的场景。

（三）韧性系统工程方法应用示例

自主机器人具有感知、决策、执行的闭环功能，通常在非结构化、动态甚至对抗性的复杂环境中执行任务，即在扰动、威胁或突发事件下仍然需要保持关键功能持续运行以完成任务。本研究以自主巡航机器人[58,75]为例，阐述韧性系统工程方法的应用过程，贯穿“韧性设计内置”思想，即在系统架构层面通过多传感器融合、容错决策等方式对韧性进行内置设计，再由形式化建模与验证来分析评估韧性设计的有效性。

1. 系统功能、性能及韧性需求分析

基于分层设计思想，将机器人软件分解为两个层次：规划决策层，完成任务规划，监控执行过程，对功能层的事件作出响应；功能层，完成机器人基本功能的执行（如图像处理、避障、运动控制等），采用模块化设计并将各项功能封装到独立的模块，由每个模块提供特定的服务和数据，相关数据由规划决策层根据当前任务读取使用。具体地，功能层中的激光测距模块将采集到的激光测距数据封装为扫描报文并存储；障碍物地图生成模块根据测距数据构建障碍物地图并形成观测报文；近程图导航（NDD）模块利用观测报文数据、定位定向管理（POM）模块生成的当前位置数据，规划出机器人路线并计算参考数据，确保机器人到达给定目标位置并可靠避障；机器人的底层执行控制（RFLEX）模块使用该参考速度，控制机器人车轮的转速并计算里程计的位置（供POM模块生成当前位置）。

机器人基于Simplex架构并集成激光与视觉导航，利用该架构的韧性保障机制[76~79]适应复杂地形、平坦地形等外部工作环境，提升机器人巡航功能的韧性能力。

2. 系统架构与结构韧性设计

采用行为–交互–优先级（BIP）建模语言及工具链[80~82]，开展自主机器人功能架构与结构韧性的设计及建模。基于BIP的系统模型构建方法将机器人的功能分解为独立的功能模块，各个模块建模作为BIP原子组件；多个原子组件通过BIP交互模型

（包括连接器和优先级）进行集成，实现各个功能模块之间的交互控制并形成复合组件，作为完整的系统功能模型。

机器人导航子系统采用Simplex架构设计以提升系统结构韧性[58]。该架构包含了两套并行导航方案：激光导航利用障碍物信息与自身位姿，视觉导航利用数字地形模型与位姿。决策模块实时监控机器人运行状态，在两套方案之间进行动态切换，并将最终控制参数下发至RFLEX模块执行。

3. 系统详细设计及单元韧性设计

以NDD功能模块为例表述基于BIP的系统详细设计、单元韧性设计的基本思路。NDD功能模块主要提供导航算法参数初始化，启动和终止给定目标的路径计算（GoTo、Stop）等服务。在BIP模型中，每个功能模块都有额外组件来接收决策层的服务请求并与模块的相应端口同步。决策层发送的请求由功能组件接收，而在服务完成后由功能组件发送报告给决策层。

NDD功能模块的BIP模型[58]包括所有组件和连接器。控制任务的周期性执行过程由原子组件进行同步，交替执行休眠和触发迁移。在1个周期内，服务组件与控制任务组件同步后完成相应动作的执行。每个功能模块都有1个服务接口，用于从决策层接收请求并返回结果。BIP模型通过连接器对复杂交互关系（如服务请求、同步、中断等）进行建模，如端口Stop.exec、GoTo.abort之间的连接器表示GoTo算法将在服务停止的时候被中断。

4. 韧性系统模型构建与模型转换

对各个功能模块的BIP组件模型进行集成，得到机器人的完整功能层详细设计模型，包括激光测距、障碍物地图生成、三维感知（P3D）、RFLEX、轨道器通信、电力与能量供给、低温环境中机器人自热、摄像头的移动控制等。

BIP框架提供基于模型转换的代码自动生成工具，可实现由BIP代码直接生成可执行的C/C++代码。整个功能层的BIP模型共有268个原子组件、1141个连接器，BIP代码生成可调用代码，用于软件功能的快速原型化和系统韧性的测试评估。

5. 系统韧性评估

BIP框架支持基于仿真的系统韧性定量评估、基于形式化验证的系统韧性定性评估。以机器人编队导航控制的防碰撞场景为例，描述基于BIP模型的机器人导航系统韧性（单元韧性）定量评估的基本思路。对于机器人存在突发故障而速度骤降的情况（可视为韧性的扰动因素），为避免目标机器人与相邻机器人发生碰撞，导航系统需要在目标机器人运动过程中始终维持一定的安全距离（可视为机器人的运动速度、加速度、摩擦系数等物理量的函数[83]）。

在相邻机器人速度骤降的情况下，验证了目标机器人的韧性导航控制算法，并在Carla仿真器中完成多个导航控制算法的BIP模型仿真测试（见图6、表4）。仿真结果表明，机器人之间的相对速度越大，在给定距离内越容易发生碰撞，即韧性越小；采用Simplex架构的混合控制器（Hybrid）的韧性指标高于其他两种控制器，应用时具有更大的韧性。

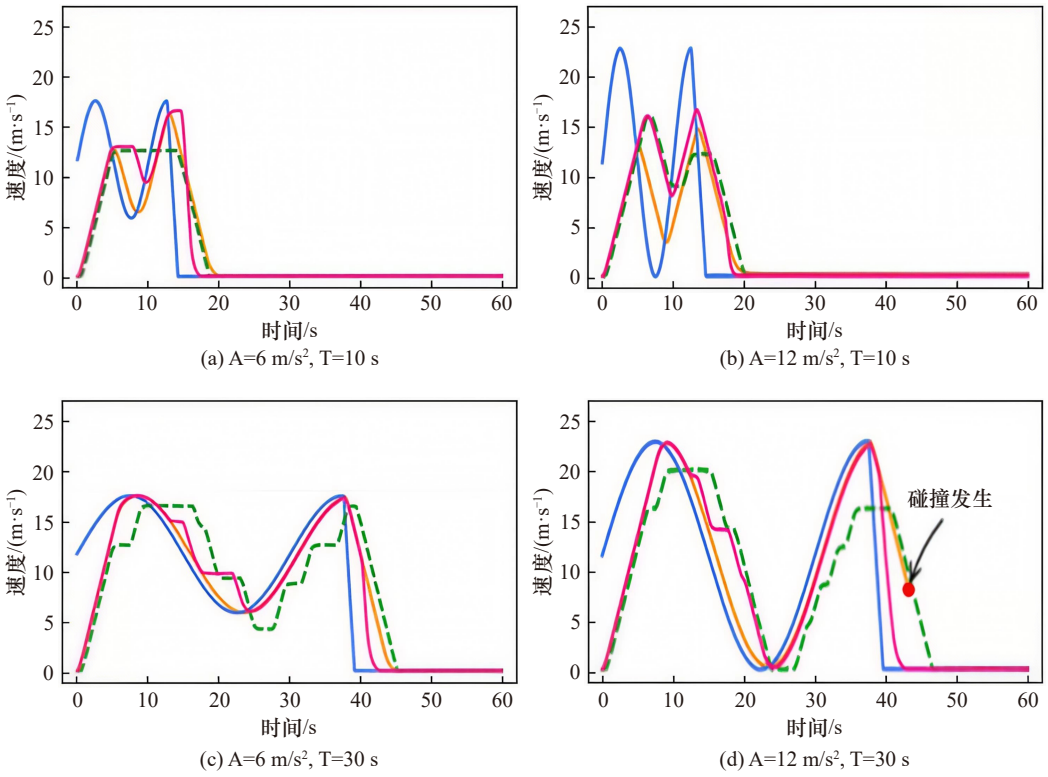
四、韧性系统工程的领域探索与面临挑战

当前，智能化转型加速发展，复杂系统愈发呈现高度互联、深度耦合、跨域集成等特征，韧性已经成为复杂系统的关键能力属性，理论与实践价值凸显。以电力能源系统、信息通信网络、无人智能系统、供应链网络为典型领域，探讨韧性理论方法的工程化探索情况，进而辨析落地应用面临的挑战。

（一）相关领域的工程化探索

1. 电力能源系统

在电力能源系统的工程实践中，对韧性能力的关注集中在实现极端条件下的能源有效供应以满足社会对能源的持续攀升需求。基于不利条件下的韧性需求分析，采用结构韧性研究思路、“分布式电源+模块化拓扑”架构设计，增强系统面对台风、冰灾等物理域不利因素时的快速恢复运行能力，保障关键负荷的电力供应[84,85]。基于单元韧性设计故障隔离子系统，确保实时感知不利条件并快速切断故障线路，防止故障影响的级联效应；结合停电时长、负荷恢复率等指标，开展数字孪生仿真，模拟各类扰动下的系统响应和优雅降级[86]。然而，在面临设备损毁、网络攻击等复杂不利条件时，现有的电力监控系统防护策略无法协同，应对智能虚假数据注入等新型威胁的能力不强，需要继续完善相关评估体系框架[87]。



(a) A=6 m/s², T=10 s　(b) A=12 m/s², T=10 s

(c) A=6 m/s², T=30 s　(d) A=12 m/s², T=30 s

图6　不同参数下的机器人导航控制的速度变化曲线

注：T、A分别表示机器人的控制周期、加速度；紫红色曲线表示Hybrid的运动轨迹；橙色曲线表示采用模型预测控制算法的NDD控制器的运动轨迹；绿色曲线表示采用阶梯控制算法的P3D控制器的运动轨迹。

表4　基于Carla仿真器的机器人导航控制的韧性定量评估结果

控制周期/s	韧性评估指标					
	A=6 m/s²			A=12 m/s²		
	NDD	P3D	Hybrid	NDD	P3D	Hybrid
10	0.22	0.25	0.5	0.17	0.26	0.38
30	0.25	0.26	0.33	0.19	0.34	0.43

2. 信息通信网络

在信息通信网络的工程实践中，韧性一般以保障服务不中断为核心目标。引入软件定义网络控制面与数据面解耦的理念，在光缆中断、设备失效时能够秒级重构网络拓扑，显现结构韧性功能解耦、拓扑重构等核心特质[88]。应用网络冗余机制，依托节点与链路备用配置，在硬件故障时自动启用备份资源，将韧性预防与恢复能力映射为确保网络连接不掉线和数据不丢失。运用虚实结合的测试评估方法，提前测试信息通信网络在极端不利条件下的韧性能力[89]。然而，当信息通信网络遭遇物理摧毁、网络攻击的混合扰动时，物理层的备用设施、信息层的加密策略难以协作；多数信息通信网络系统韧性恢复机制无法应对未知风险（如零日漏洞），通用评估方法也难以覆盖从预防到演进的全流程[90,91]。

3. 无人智能系统

无人智能系统的韧性主要以完成使命任务、按需提供功能服务为目标。针对无人智能系统的协同控制，通常采用模块化架构、冗余配置等方式实现系统的结构韧性和特定模组的单元韧性。采取架构驱动设计、结构韧性嵌入的方式，确保无人智能系统在部分节点受扰失效时能够根据预设重构策略，实现功能适配与性能恢复[92]。针对感知硬件缺陷引发的异常情况，快速切换感知模态，将抵御与恢复能力转化为应用实效[93]。引入数字孪生技术构建虚实融合的智能测试环境，辅助开展无人智能系统的韧性设计、评估和验证[94]。然而，无人智能系统的现有系统设计主要关注预设场景和已知的不利条件，针对未知扰动或不利条件的自主学习与能力演进机制尚不成熟；也需探索考虑具体任务时效性、集群规模效应等特征与韧性的关系，继续完善相关的度量框架[95]。

4. 供应链网络

在供应链韧性管理方面，2004年首次阐述了供应链韧性的概念内涵，即在受到某种干扰后供应链能够快速恢复甚至提升运营状态的能力[96]。后续研究提出，供应链韧性不仅应具备抵抗能力、恢复能力，而且应具有生存发展能力[97]；可将供应链韧性管理概括为中断发生前积极的想法和计划、中断发生时保持对供应链结构和功能的控制、中断发生后快速有效的恢复措施[98]。也有研究认为，供应链韧性管理应侧重供应链在发生中断时持续存在或转变的动态能力，以使企业在遭受外部冲击或转型中能够维持运营、在面临意外中断时可以有序恢复[99]。在实践层面，将区块链技术应用到供应链架构，支持创建高效、互信、安全、智能的供应链韧性管理系统[100]；物联网与云计算协同并在供应链网络内实现互联互通，通过外部物联网技术结构、内部供应链组织架构、专有云计算系统获取实时的供需数据，增强风险来临时的供应链韧性[101]；发展了供应链风险管理数字化概念，通过集成、共享、处理供应链网络上的实时风险信息，增强供应链风险识别、分析、评估、缓解、监控过程的韧性、智能性与可控力[102]。整体上，供应链韧性已从早期强调灾后恢复能力发展为涵盖抵抗、适应、演进能力的综合性概念，融合区块链、物联网、数字化平台等前沿技术，构建透明、互信、实时互联的供应链网络，实质性提升对风险的智能预警与协同响应能力，推动风险管理向数字化、智能化演进。也要注意到，相关研究面临着理论与现实的衔接困境：供应链韧性的概念内涵、衡量标准等尚未统一，难以精确评估应用有效性、投资回报率等；数字技术与现有的组织架构、业务流程进行融合，克服伴生的成本与复杂性也是现实挑战。

（二）落地应用面临的挑战

1. 韧性理论框架有待扩充和统一

国内外虽已提出多种韧性定义与方法论，但不同学科领域之间的表述存在显著的差异[103]。系统工程层面的通用理论框架仍显缺乏，韧性理论要素嵌入系统全生命周期过程面临直接挑战。当前的工程实践多为单一系统的韧性优化，而在“系统之系统”的韧性设计方面缺乏有效的工具与方法。例如，能源电力、智慧交通等复杂系统涉及多领域的技术栈和软硬件运行平台，属于高度异构的“系统之系统”，亟需在统一的概念模型和理论框架下，探索解决复杂系统或体系韧性的全生命周期设计与跨域集成难题。

2. 不同系统的韧性度量评估存在较大差异

电力能源系统以平均恢复时长为核心指标，信息通信网络侧重网络连通度，无人智能系统关注持续提供关键功能的自主性，各类系统的韧性度量评估重点呈明显的差异化。当前的工程实践缺少跨领域、可操作的度量评估框架，导致系统韧性评估指标与方法不便跨域应用和推广；也较多依赖事后评估，难以支撑实时监测和动态优化。亟需运用模型驱动工程、数字孪生等技术手段，建立多层次、可量化的通用韧性评估体系。

3. 系统复杂性、威胁多样性引发韧性建模与分析困境

系统的跨域特征既导致系统复杂度提高，也加剧不同维度扰动或不利条件的交织、叠加、级联等影响。这种影响具有非线性、不确定性、多尺度等特性，对系统韧性建模构成直接挑战[104]。当前的韧性建模多采用线性化模型，难以捕捉系统全局的动态行为，无法刻画非线性特征引起的微小扰动引发系统行为突变。亟需深化复杂系统理论研究，破解非线性、不确定性、多尺度建模难题。

4. 多目标优化设计复杂度高

韧性能力的维持和演进需以合理的资源冗余作为依托，而降低资源成本、提高研制效率又是系统能否完成使命任务的重要考量。韧性系统工程强调在系统韧性设计、实施、演进过程中对成本效率、功能 / 性能、韧性能力等多类目标进行权衡。当前的工程实践主要以完成系统的功能、性能为首要目标，可以兼顾成本效率，但对韧性能力的考虑存在明显不足。复杂系统的高度互联、深度耦合、跨域集成等特征进一步加剧多目标协同优化设计的复杂性，成为韧性系统工程化实施的重大挑战[105]。

5. AI对韧性系统工程实践构成新挑战

AI可为复杂系统赋能，但也显著增加系统功能架构的复杂度和不确定性[106]。AI算法具有“黑盒”特性、面临对抗样本攻击的脆弱性、幻觉等问题，遭受概念漂移（数据分布变化导致模型性能退化[107]）、对抗攻击（规避攻击、数据投毒、模型窃取等[108]）、故障注入（硬件瞬态错误、激光攻击

等[109]）等不利条件影响的范围与演化路径难以预测。亟需探究面向AI特别是大模型的韧性机理，从系统工程的角度构建智能系统的韧性保障理论体系和方法框架。

五、结语

本文围绕韧性系统工程的核心问题，系统分析了韧性的概念内涵、扰动因素、能力阶段、属性差异，提出了韧性系统工程的定义、方法流程、评估框架。在理论方法层面，拓展了传统的系统工程“V”模型，将预防、抵御、适应、恢复、演进等韧性能力贯穿系统全生命周期的设计、验证、评估活动中。在评估体系方面，构建了覆盖定量评估、定性评估的韧性指标框架。在应用探索方面，给出了韧性系统工程方法应用示例，结合电力能源系统、信息通信网络、无人智能系统等典型复杂系统场景，探讨了韧性系统工程的实践路径以及落地应用面临的潜在挑战。韧性系统工程将确保完成使命任务作为首要目标，突破了传统系统工程面向功能、性能、成本与进度平衡的局限，并以“韧性设计内置”的理念推动系统工程从事后防御转向动态适应与自主演进发展。

面向未来，韧性系统工程仍需在若干方向深化研究与拓展应用。建立统一的韧性度量与评估方法，以解决不同任务场景下指标体系分散且标准化不足的问题。研究面向多域扰动的建模与分析方法，尤其是引入AI、数字孪生等信息技术，以提升复杂系统韧性设计的科学性与可验证性。探索包括成本、效率、韧性在内的多目标优化决策方法，以兼顾实际工程约束与长期演进需求。重视智能化、无人化背景下的风险演进态势，尤其是AI脆弱性、跨域协同机理缺失等引发的新型挑战。通过持续的理论创新、方法完善、工程实践，将韧性系统工程发展成为系统工程的新范式，为关键基础设施、智能无人装备、复杂系统的安全可靠运行与持续适应演进提供坚实的理论方法支撑。

利益冲突声明

本文作者在此声明不存在任何利益冲突或财务冲突。

Received date: August 24, 2025; **Revised date:** December 12, 2025

Corresponding author: Yang Lin is a research fellow from the Systems Engineering Research Institute, Academy of Military Sciences. His major research fields include cyber security and systems engineering. E-mail: yanglin61s@sina.com

Funding project: Key Project of the Foundation Enhancement Program (2025-JCJQ-ZD-015-00); Comprehensive Research Project (JK2023B010300-4)

参考文献

[1] Lou S H, Hu Z X, Zhang Y R, et al. Human–cyber–physical system for industry 5.0: A review from a human-centric perspective [J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 494–511.

[2] Walker B, Holling C S, Carpenter S R, et al. Resilience, adaptability and transformability in social–ecological systems [J]. Ecology and Society, 2004, 9(2): 5.

[3] Folke C. Resilience: The emergence of a perspective for social–ecological systems analyses [J]. Global Environmental Change, 2006, 16(3): 253–267.

[4] 黄浪, 吴超, 杨冕, 等. 韧性理论在安全科学领域中的应用 [J]. 中国安全科学学报, 2017, 27(3): 1–6.
Huang L, Wu C, Yang M, et al. Application of resilience theory in field of safety science [J]. China Safety Science Journal, 2017, 27(3): 1–6.

[5] Holling C S. Resilience and stability of ecological systems [J]. Annual Review of Ecology and Systematics, 1973, 4 (1973): 1–23.

[6] INCOSE. Resilient systems working group: Working to deliver capability when faced with adverse conditions [EB/OL]. (2024-10-09)[2025-12-15]. https://www.incose.org/communities/working-groups-initiatives/resilient-systems.

[7] Bodeau D, Graubart R, Picciotto J, et al. Cyber resiliency engineering framework [EB/OL]. (2011-09-01)[2025-12-15]. https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-framework.

[8] Bodeau D, Graubart R, Heinbockel W. et al. Cyber resiliency engineering aid—The updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques [EB/OL]. (2015-05-01)[2025-12-15]. https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-aid-updated-cyber-resiliency-engineering.

[9] National Institute of Standards and Technology. Developing cyber-resilient systems: A systems security engineering approach [R]. Gaithersburg: National Institute of Standards and Technology, 2021.

[10] Official Journal of the European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council [EB/OL]. (2024-11-20)[2025-12-15]. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[11] INCOSE. INCOSE systems engineering handbook [M]. New York: John Wiley & Sons, 2023.

[12] Hollnagel E, Woods D D, Leveson N. Resilience engineering: Concepts and precepts [M]. London: CRC Press, 2006.

[13] Hosseini S, Barker K, Ramirez-Marquez J E. A review of definitions and measures of system resilience [J]. Reliability Engineering & System Safety, 2016, 145: 47–61.

[14] Madni A M, Jackson S. Towards a conceptual framework for resilience engineering [J]. IEEE Systems Journal, 2009, 3(2): 181–191.
[15] Thompson M A, Ryan M J, Slay J, et al. A new resilience taxonomy [J]. INCOSE International Symposium, 2016, 26(1): 1318–1330.
[16] Tsigkanos C, Nastic S, Dustdar S. Towards resilient Internet of things: Vision, challenges, and research roadmap [R]. Dallas: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019.
[17] Berger C, Eichhammer P, Reiser H P, et al. A survey on resilience in the IoT: Taxonomy, classification, and discussion of resilience mechanisms [J]. ACM Computing Surveys, 2022, 54(7): 1–39.
[18] Brtis J S, McEvilley M A. Systems engineering for resilience [R]. San Diego: MITRE Corporation, 2019.
[19] Bishop M, Carvalho M, Ford R, et al. Resilience is more than availability [R]. Marin County: 2011 New Security Paradigms Workshop, 2011.
[20] Clark A, Zonouz S. Cyber-physical resilience: Definition and assessment metric [J]. IEEE Transactions on Smart Grid, 2019, 10(2): 1671–1684.
[21] 潘星, 蒋卓, 杨艳京. 基于弹性的体系组件重要度及恢复策略 [J]. 北京航空航天大学学报, 2017, 43(9): 1713–1720.
Pan X, Jiang Z, Yang Y J. Resilience-based component importance and recovery strategy for system-of-systems [J]. Journal of Beijing University of Aeronautics and Astronautics, 2017, 43(9): 1713–1720.
[22] Laprie J C. From dependability to resilience [R]. Anchorage: The 38th IEEE/IFIP International Conference on Dependable Systems and Networks, 2008.
[23] Linkov I, Eisenberg D A, Plourde K, et al. Resilience metrics for cyber systems [J]. Environment Systems and Decisions, 2013, 33(4): 471–476.
[24] Kott A, Linkov I. Cyber resilience of systems and networks [M]. Cham: Springer International Publishing, 2019.
[25] Delic K A. On resilience of IoT systems [J]. Ubiquity, 2016, 2: 1–7.
[26] Laxman N, Krohmer D, Damm M, et al. Understanding resilience: Looking at frameworks & standards—A systematic study from cyber perspective [R]. Venice: 2023 IEEE International Conference on Cyber Security and Resilience (CSR), 2023.
[27] Alhidaifi S M, Asghar M R, Ansari I S. A survey on cyber resilience: Key strategies, research challenges, and future directions [J]. ACM Computing Surveys, 2024, 56(8): 1–48.
[28] Segovia-Ferreira M, Rubio-Hernan J, Cavalli A, et al. A survey on cyber-resilience approaches for cyber-physical systems [EB/OL]. (2023-02-10)[2025-12-15]. https://arxiv.org/abs/2302.05402.
[29] Sterbenz J P G, Hutchison D, Çetinkaya E K, et al. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines [J]. Computer Networks, 2010, 54(8): 1245–1265.
[30] Liu X M, Li D Q, Ma M Q, et al. Network resilience [J]. Physics Reports, 2022, 971: 1–108.
[31] Najjar W, Gaudiot J L. Network resilience: A measure of network fault tolerance [J]. IEEE Transactions on Computers, 1990, 39(2): 174–181.
[32] Erdene-Ochir O, Kountouris A, Minier M, et al. A new metric to quantify resiliency in networking [J]. IEEE Communications Letters, 2012, 16(10): 1699–1702.
[33] Chacon-Chamorro M, Felipe G L, Quijano N, et al. Cooperative resilience in artificial intelligence multiagent systems [J]. IEEE Transactions on Artificial Intelligence, 2025, 6(12): 3430–3440.
[34] Avizienis A, Laprie J C, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11–33.
[35] Jeffery A, Howard H, Mortier R. Rearchitecting kubernetes for the edge [R]. Online: The 4th International Workshop on Edge Systems, Analytics and Networking, 2021.
[36] Henry D, Emmanuel R M J. Generic metrics and quantitative approaches for system resilience as a function of time [J]. Reliability Engineering & System Safety, 2012, 99: 114–122.
[37] Çetinkaya E K, Broyles D, Dandekar A, et al. Modelling communication network challenges for future Internet resilience, survivability, and disruption tolerance: A simulation-based approach [J]. Telecommunication Systems, 2013, 52(2): 751–766.
[38] Thoma K, Scharte B, Hiller D, et al. Resilience engineering as part of security research: Definitions, concepts and science approaches [J]. European Journal for Security Research, 2016, 1(1): 3–19.
[39] Patriarca R, Bergström J, Gravio G, et al. Resilience engineering: Current status of the research and future challenges [J]. Safety Science, 2018, 102: 79–100.
[40] Hall A D. A methodology for systems engineering [J]. Research Management, 1962, 8(1): 56–58.
[41] Checkland P. Systems thinking, systems practice [M]. New York: John Wiley & Sons, 1981.
[42] Sage A P. Systems engineering [M]. New York: John Wiley & Sons, 1992.
[43] Blanchard B S, Fabrycky W J. Systems engineering and analysis [M]. Englewood Cliffs: Prentice-Hall, 1981.
[44] Madni A M, Sievers M. Model-based systems engineering: Motivation, current status, and research opportunities [J]. Systems Engineering, 2018, 21(3): 172–190.
[45] Baxter G, Sommerville I. Socio-technical systems: From design methods to systems engineering [J]. Interacting with Computers, 2011, 23(1): 4–17.
[46] 钱学森, 许国志, 王寿云. 组织管理的技术——系统工程 [N]. 文汇报, 1978-09-27(01).
Qian X S, Xu G Z, Wang S Y. Systems engineering: A technology for organization and management [N]. Wenhui Daily, 1978-09-27(01).
[47] 钱学森. 论系统工程 [M]. 长沙: 湖南科学技术出版社, 1988.
Qian X S. On systems engineering [M]. Changsha: Hunan Science and Technology Press, 1988.
[48] 苗东升. 钱学森与系统科学 [J]. 中国工程科学, 2001, 3(8): 1–6.
Miao D S. Qian Xuesen and system science [J]. Strategic Study of CAE, 2001, 3(8): 1–6.
[49] 王众托. 创建知识系统工程学科 [J]. 中国工程科学, 2006, 8(12): 1–9.

Wang Z T. Establishing a new discipline: Knowledge systems engineering [J]. Strategic Study of CAE, 2006, 8(12): 1–9.

[50] 郭宝柱. 大型复杂技术项目的系统观点与系统工程方法 [J]. 中国工程科学, 2008, 10(3): 25–30.
Guo B Z. Systems engineering in large complex technical projects [J]. Strategic Study of CAE, 2008, 10(3): 25–30.

[51] 董超华, 杨忠东, 施进明, 等. 系统工程方法在风云三号极轨气象卫星地面应用系统工程中的应用 [J]. 中国工程科学, 2013, 15(10): 24–32.
Dong C H, Yang Z D, Shi J M, et al. Systematic engineering method for FY-3 satellite ground segment engineering [J]. Strategic Study of CAE, 2013, 15(10): 24–32.

[52] 党炜, 许鹏程, 郑作环, 等. 价值可持续太空探索的系统工程——理念、架构与实践 [J]. 中国工程科学, 2025, 27(3): 229–246.
Dang W, Xu P C, Zheng Z H, et al. Systems engineering for value-sustainable space exploration: Philosophy, architecture, and practice [J]. Strategic Study of CAE, 2025, 27(3): 229–246.

[53] 杨为民, 阮镰, 屠庆慈. 可靠性系统工程——理论与实践 [J]. 航空学报, 1995, 16(S1): 1–8.
Yang W M, Ruan L, Tu Q C. Reliability system engineering—Theory and practice [J]. Acta Aeronautica et Astronautica Sinica, 1995, 16(S1): 1–8.

[54] 康锐, 王自力. 可靠性系统工程的理论与技术框架 [J]. 航空学报, 2005, 26(5): 633–636.
Kang R, Wang Z L. Framework of theory and technique about reliability system engineering [J]. Acta Aeronautica et Astronautica Sinica, 2005, 26(5): 633–636.

[55] 任羿, 王自力, 杨德真, 等. 基于模型的可靠性系统工程 [M]. 北京: 国防工业出版社, 2021.
Ren Y, Wang Z L, Yang D Z, et al. Model based reliability systems engineering [M]. Beijing: National Defense Industry Press, 2021.

[56] 康锐, 王自力. 可靠性系统工程理论研究回顾与展望 [J]. 航空学报, 2022, 43(10): 527505.
Kang R, Wang Z L. Reliability systems engineering: A research review and prospect [J]. Acta Aeronautica et Astronautica Sinica, 2022, 43(10): 527505.

[57] Jackson S, Ferris T L J. Resilience principles for engineered systems [J]. Systems Engineering, 2013, 16(2): 152–164.

[58] Joseph S. Rigorous system design [EB/OL]. (2012-04-15)[2025-12-15]. https://www-verimag. imag. fr/~sifakis/papers_pdfs/Rigorous%20System%20Design.pdf.

[59] Verma D. Systems engineering for the digital age: Practitioner perspectives [M]. New York: John Wiley & Sons, 2023.

[60] Nardi L, Koeplinger D, Olukotun K. Practical design space exploration [R]. Rennes: 2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), 2019.

[61] Ayyub B M. Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making [J]. Risk Analysis, 2014, 34(2): 340–355.

[62] Bruneau M, Chang S E, Eguchi R T, et al. A framework to quantitatively assess and enhance the seismic resilience of communities [J]. Earthquake Spectra, 2003, 19(4): 733–752.

[63] Reed D A, Kapur K C, Christie R D. Methodology for assessing the resilience of networked infrastructure [J]. IEEE Systems Journal, 2009, 3(2): 174–180.

[64] Ouyang M, Dueñas-Osorio L. Time-dependent resilience assessment and improvement of urban infrastructure systems [J]. Chaos, 2012, 22(3): 033122.

[65] Francis R, Bekera B. A metric and frameworks for resilience analysis of engineered and infrastructure systems [J]. Reliability Engineering & System Safety, 2014, 121: 90–103.

[66] Fang Y P, Pedroni N, Zio E. Resilience-based component importance measures for critical infrastructure network systems [J]. IEEE Transactions on Reliability, 2016, 65(2): 502–512.

[67] Ganin A A, Massaro E, Gutfraind A, et al. Operational resilience: Concepts, design and analysis [J]. Scientific Reports, 2016, 6: 19540.

[68] Mishra S, Rao A, Krishnan R, et al. Reliability, resilience and human factors engineering for trustworthy AI systems [EB/OL]. (2024-11-13)[2025-12-15]. https://arxiv.org/abs/2411.08981.

[69] Cao X Y, Feng D C. Probabilistic resilience assessment framework of structures considering the combined functionality-recovery-duration uncertainty [J]. Mechanical Systems and Signal Processing, 2025, 223: 111856.

[70] Li Z S, Wu G Y, Cassandro R, et al. A review of resilience metrics and modeling methods for cyber-physical power systems (CPPS) [J]. IEEE Transactions on Reliability, 2024, 73(1): 59–66.

[71] Nan C, Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures [J]. Reliability Engineering & System Safety, 2017, 157: 35–53.

[72] Feng Q, Liu M, Dui H Y, et al. A general design-oriented resilience measurement and evaluation method for engineering systems: Resilience cube [J]. Reliability Engineering & System Safety, 2024, 245: 110038.

[73] Beling P, Horowitz B, McDermott T. Developmental test and evaluation (DTE&A) and cyberattack resilient systems [R]. Hoboken: Systems Engineering Research Center, 2021.

[74] Liu C, Xu F L, Gao C, et al. Deep learning resilience inference for complex networked systems [J]. Nature Communications, 2024, 15: 9203.

[75] Abdellatif T, Bensalem S, Combaz J, et al. Rigorous design of robot software: A formal component-based approach [J]. Robotics and Autonomous Systems, 2012, 60(12): 1563–1578.

[76] Sha L. Using simplicity to control complexity [J]. IEEE Software, 2001, 18(4): 20–28.

[77] Chen S D, Sun Y W, Li D C, et al. Runtime safety assurance for learning-enabled control of autonomous driving vehicles [R]. Philadelphia: 2022 International Conference on Robotics and Automation (ICRA), 2022.

[78] Wang Q, Kou G, Chen L Q, et al. Runtime assurance of learning-based lane changing control for autonomous driving vehicles [J]. Journal of Circuits, Systems and Computers, 2022, 31(14): 2250249.

[79] 王强, 陈强, 曹伟朋, 等. 基于单工架构的信息物理系统运行时安全性保障方法 [J]. 深圳大学学报(理工版), 2024, 41(3): 253–263.
Wang Q, Chen Q, Cao W P, et al. Runtime safety assurance methods for cyber physical systems based on simplex architecture [J].

Journal of Shenzhen University (Science and Engineering), 2024, 41(3): 253–263.

[80] Basu A, Bensalem B, Bozga M, et al. Rigorous component-based system design using the BIP framework [J]. IEEE Software, 2011, 28(3): 41–48.

[81] Bliudze S, Cimatti A, Jaber M, et al. Formal verification of infinite-state BIP models [R]. Cham: Automated Technology for Verification and Analysis, 2015

[82] Konnov I, Kotek T, Wang Q, et al. Parameterized systems in BIP: Design and model checking [R]. Québec City: The 27th International Conference on Concurrency Theory, 2016.

[83] Wang Q, Zheng X L, Zhang J Y, et al. A hybrid controller for safe and efficient longitudinal collision avoidance control [J]. Journal of Systems Architecture, 2022, 125: 102432.

[84] Liu Y L, Feng H N, Hatziargyriou N D. Multi-stage collaborative resilient enhancement strategy for coupling faults in distribution cyber physical systems [J]. Applied Energy, 2023, 348: 121560.

[85] Kostenko G, Zaporozhets A. Enhancing of the power system resilience through the application of micro power systems (microgrid) with renewable distributed generation [J]. System Research in Energy, 2023 (3): 25–38.

[86] Bitencourt J, Wooley A, Harris G. Verification and validation of digital twins: A systematic literature review for manufacturing applications [J]. International Journal of Production Research, 2025, 63(1): 342–370.

[87] Huang H, Vincent Poor H, Davis K R, et al. Toward resilient modern power systems: From single-domain to cross-domain resilience enhancement [J]. Proceedings of the IEEE, 2024, 112(4): 365–398.

[88] Malik A, de Fréin R, Aziz B, et al. Rapid restoration techniques for software-defined networks [J]. Applied Sciences, 2020, 10(10): 3411.

[89] Peuster M, Schneider S, Zhao M X, et al. Introducing automated verification and validation for virtualized network functions and services [J]. IEEE Communications Magazine, 2019, 57(5): 96–102.

[90] 东润泽, 王布宏, 张杰勇, 等. 面向通信感知一体化的无人机集群上行链路物理层安全传输 [J]. 信号处理, 2025, 41(7): 1143–1152.
Dong R Z, Wang B H, Zhang J Y, et al. Physical layer security for UAV swarm uplink transmission with integrated sensing and communication [J]. Journal of Signal Processing, 2025, 41(7): 1143–1152.

[91] Guo M Z, Lin Z, Ma R Q, et al. Inspiring physical layer security with RIS: Principles, applications, and challenges [J]. IEEE Open Journal of the Communications Society, 2024, 5: 2903–2925.

[92] Guo L, Yu X, Zhang X, et al. Safety control system technologies for UAVs: Review and prospect [J]. Scientia Sinica Informationis, 2020, 50(2): 184–194.

[93] Dui H Y, Wang X Y, Zhou H H, et al. Redundancy-based resilience optimization of multi-component systems [J]. Mathematics, 2023, 11(14): 3151.

[94] Meng Z J, Zhao S L, Chen H, et al. The vehicle testing based on digital twins theory for autonomous vehicles [J]. IEEE Journal of Radio Frequency Identification, 2022, 6: 710–714.

[95] 江碧涛, 温广辉, 周佳玲, 等. 智能无人集群系统跨域协同技术研究现状与展望 [J]. 中国工程科学, 2024, 26(1): 117–126.
Jiang B T, Wen G H, Zhou J L, et al. Cross-domain cooperative technology of intelligent unmanned swarm systems: Current status and prospects [J]. Strategic Study of CAE, 2024, 26(1): 117–126.

[96] Christopher M, Lee H. Mitigating supply chain risk through improved confidence [J]. International Journal of Physical Distribution & Logistics Management, 2004, 34(5): 388–396.

[97] Nasir S B, Ahmed T, Karmaker C L, et al. Supply chain viability in the context of COVID-19 pandemic in small and medium-sized enterprises: Implications for sustainable development goals [J]. Journal of Enterprise Information Management, 2022, 35(1): 100–124.

[98] Kamalahmadi M, Parast M M. A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research [J]. International Journal of Production Economics, 2016, 171: 116–133.

[99] Wieland A, Durach C F. Two perspectives on supply chain resilience [J]. Journal of Business Logistics, 2021, 42(3): 315–322.

[100] Azzi R, Chamoun R K, Sokhn M. The power of a blockchain-based supply chain [J]. Computers & Industrial Engineering, 2019, 135: 582–592.

[101] Kranz M. Success with the Internet of things requires more than chasing the cool factor [J]. Harvard Business Review, 2017, 3: 1–10.

[102] Schuster E W, Brock D L, Allen S J. Global RFID: The value of the EPC global network for supply chain management [M]. Berlin: Springer, 2007.

[103] Krakovská H, Kuehn C, Longo I P. Resilience of dynamical systems [J]. European Journal of Applied Mathematics, 2024, 35(1): 155–200.

[104] Wang H D, Yan H, Rong C, et al. Multi-scale simulation of complex systems: A perspective of integrating knowledge and data [J]. 2024, 56(12): 1–38.

[105] 郭明雪, 赵婷婷, 高自友. 韧性背景下道路交通网络保护和修复优化方法综述 [J]. 系统工程理论与实践, 2024, 44(11): 3626–3638.
Guo M X, Zhao T T, Gao Z Y. Review of optimization methodologies for road transportation network protection and restoration to enhance system resilience [J]. Systems Engineering—Theory & Practice, 2024, 44(11): 3626–3638.

[106] Wells E M, Boden M, Tseytlin I, et al. Modeling critical infrastructure resilience under compounding threats: A systematic literature review [J]. Progress in Disaster Science, 2022, 15: 100244.

[107] Agrahari S, Singh A K. Concept drift detection in data stream mining: A literature review [J]. Journal of King Saud University – Computer and Information Sciences, 2022, 34(10): 9523–9540.

[108] Zhou S, Liu C, Ye D Y, et al. Adversarial attacks and defenses in deep learning: From a perspective of cybersecurity [J]. 2022, 55(8): 1–39.

[109] Malekzadeh E, Rohbani N, Lu Z H, et al. The impact of faults on DNNs: A case study [R]. Athens: 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2021.