doi: 10.3969/j.issn.2097-0358.2024.01.006

基于 STPA 方法的智能船航行风险评价指标体系构建

李 伟[1,2]，郭云龙[1]，郭兴华[1]，夏红兵[1]

（1. 江苏航运职业技术学院 航海技术学院，江苏 南通 226010；2. 上海海事大学 商船学院，上海 201306）

摘 要：针对智能船航行安全风险致因辨识问题，基于 STAMP 理论，构建基于船员功能替代的智能船系统模型。将船舶航行风险视为系统安全控制问题，运用 STPA 方法进行风险致因因素分析，在此基础上从组分失效、外部环境干扰和不安全交互三个维度构建智能船航行风险评价指标体系。该指标体系涵盖要素广、风险针对性强，能够科学客观地表征船舶航行系统的安全状态，相关成果为后续开展智能船航行风险定量化评估工作奠定了基础。

关键词：智能船；风险分析；STAMP；STPA；风险指标

中图分类号：U664.82 **文献标志码**：A **文章编号**：2097-0358(2024)1-0029-06

0 引言

伴随工业 4.0 时代的到来，自动控制技术、人工智能、互联网及通信技术的发展有力地推动了船舶智能化，使船舶航行向自主化发展。业界普遍认为智能船在降低人因素引发的航行事故、降低运营成本和促进节能减排等诸多方面具有突出优势，其研发和应用已成为促进航运发展的新动力、新热点。[1-2]“至少应不低于传统人工控制船舶的安全水平”这一标准已在业界达成了广泛的共识。围绕智能船安全性问题，目前在船舶设计、智能避碰、导航及控制等关键技术方面均取得了较大突破，小型自主货船实船测试已在特定水域内展开。针对智能船的营运风险，学者们已开展一系列前瞻性研究，并取得初步成果，但由于缺乏实船数据，已有成果多依赖专家经验或在普通货船事故案例基础上基于专家头脑风暴的定性分析。Wróbel 等通过对 100 份海事事故报告分析得出，随着智能船舶的发展，出现碰撞、搁浅等航行事故的概率有望降低，而一旦出现火灾、船舶结构受损等非航行事故，由于人员无法及时介入，由此所造成事故后果可能会更加严重。[3]Rødseth 等指出，船舶设备（硬件和软件）的可靠性是智能船安全运行的主要因素。[4]段尊雷等认为，影响智能船舶安全的因素应包括，船舶设备（硬件和软件）的可靠性，设计人员、岸基操作人员错误或失误的关联影响，网络通信的因素，信息传输和软件安全性，货物管理和应急管理等。[5]张文君等提出了基于等级全息建模的风险辨识方法，从人、机、环、管四个维度对智能船航行风险影响因素进行辨识。[6]

前期研究重点对人因素、通信网络、系统关键设备、环境干扰等影响船舶航行安全的关键因素完成初步辨识，但对系统交联、组分交互作用带来的船舶风险致因辨识研究不足。智能船是一个新兴的复杂装备系统，船舶的数字化和软件密集化特征使得系统、子系统间非线性关联及交互作用显著增强[7]，船舶航行风险构成和作用机制更加复杂，迫切需要基于系统理论的视角，构建智能船航行安全评价指标体系，以推动船舶航行风险定量化研究，为尚处于早期发展阶段的智能船航行安全风险防控提供指导。

传统风险分析方法多以可靠性理论为基础，并假定系统间为相对简单的逻辑关联或较为显性因果关系，这显然不适于直接用于智能船的风险研究，亟需采用基于系统理论的方法进行建模。基于系统理论事故建模与过程模型（Systems-Theoretic Accident Modeling and Processes，STAMP）源于系统理论和控制理论，具有强大的建模能力，能够充分描述组分间的交互、约束与控制关系，对复杂系统的风险分析有着显著优势，已被广泛应用于航空、铁路运输等领域风险分析[8-9]。基于此，本文将结合 STAMP 理论，构建基于船员功能替

收稿日期：2024-03-03

基金项目：南通市科技计划基础科学研究面上项目（JC22022062）

作者简介：李伟（1984— ），男，山东枣庄人，江苏航运职业技术学院航海技术学院副教授，上海海事大学商船学院博士生。

代的智能船系统模型，并进一步采用 STPA 方法进行安全性分析，探索智能船航行风险评价指标体系的构建方法，以推动船舶航行风险的定量化研究。

1 STAMP 模型/STPA 方法

Leveson 教授于 2004 年提出 STAMP 模型，以更加全面地分析和解决社会技术复杂系统的事故致因问题。[10]不同于以往的安全性分析方法，该模型把复杂系统的安全性分析当作一个控制问题，认为安全性是复杂系统的涌现特性，安全管理的焦点也从提高组件可靠性、减少故障率转变为加强对系统行为的约束。通过建模分析可捕获系统内部功能关系和交互过程，约束、分层控制结构和过程模型是 STAMP 模型三个基本的要素。

STPA（Systems Theoretic Process Analysis，STPA）方法是基于 STAMP 模型的系统性安全评估方法，其实施基本步骤如图 1 所示。STPA 是一种自上而下的分析方法，其构建的是一个由功能控制图组成的系统模型，而不是传统的危险分析方法所使用的物理组件图，旨在通过构建由传感器、控制器、执行器和控制过程构成的反馈回路，捕获系统内部功能关系和交互过程，辨识不安全的控制行为及损失场景。

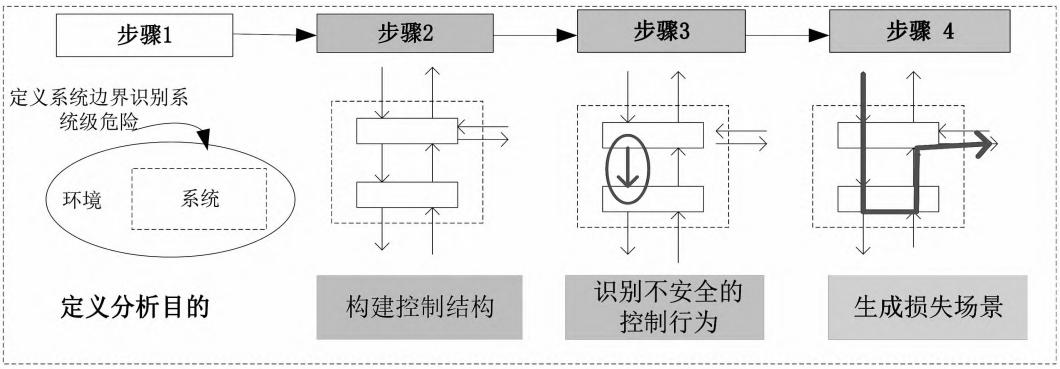

图 1 STPA 方法分析步骤

与传统的危害分析技术相比，STPA 在识别安全要求方面可以更精确，因为这些约束是从每个因果关系和危险场景中识别出来的，特别是那些与软件、系统设计和人类行为相关的约束。STPA 定义了 4 种不安全控制行为，分别为：(1)没有提供所需要的安全控制行为(或提供正确的控制指令但没有被实施)；(2)提供的控制行为是错误的或不安全的；(3)提供了正确的控制行为，但出现控制行为发生了延迟；(4)提供了正确的控制行为，但作用时间不匹配，结束时间过早或过晚。

根据以上 4 种不安全控制行为，通过对具体场景中系统损失的致因场景分析，结合系统安全约束传递过程，将控制回路映射到具体的物理组件，通过细化组件间约束关系，可辨识出导致不安全控制行为的具体原因，进一步归纳总结即可得到影响智能船航行安全的风险因素，从而构建出航行风险致因的评价指标体系，开展智能船航行风险评估。

2 基于 STPA 方法的智能船航行风险致因分析

2.1 定义分析目的

本文研究对象为远程控制智能船，由此确定系统研究的边界为远程控制智能船安全航行，分析目标为识别航行风险及风险场景，以采取针对性控制措施，减小或降低风险发生概率。根据远程控制船航行期间控制主体的不同，确定船岸协同控制的航行场景包括：(1)以船载自主系统(Autonomous Control of Ship-based Systems，ASC)为主导的自主驾驶模式；(2)以岸基中心(Shore based Control Center，SCC)系统作业人员为主导的远程控制模式，船舶航行期间可能造成的风险损失有船舶碰撞、船舶搁浅、船舶失控以及货物损失等。根据系统研究边界和分析目标可确定系统级的危险及安全约束，进一步根据 STPA 方法分析流程，可通过分层控制结构构建、不安全行为和场景分析、风险致因因素归纳等步骤开展深入研究。

2.2 分层控制结构构建

智能船的发展仍处于早期阶段，厘清相关系统构成及作用机制，是识别智能船航行风险的关键。通过船载智能系统替代船员操作，消除人为因素的影响，实现完全自主驾驶是智能船发展的终极目标，因此需要从

实现船员功能替代的视角进行建模。基于系统理论和层次原则,充分考虑 STCW 公约(International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers)对船员职能的规定及《智能船舶规范》相关要求,并综合前期 MUNIN 项目和 AAWA 项目主要研究成果[4]360,在明确各系统或子系统的功能与船员职能任务一一对应的基础上,按照系统分层控制的逻辑,构建出基于船员功能替代的自主船系统 STAMP 模型,如图 2 所示。

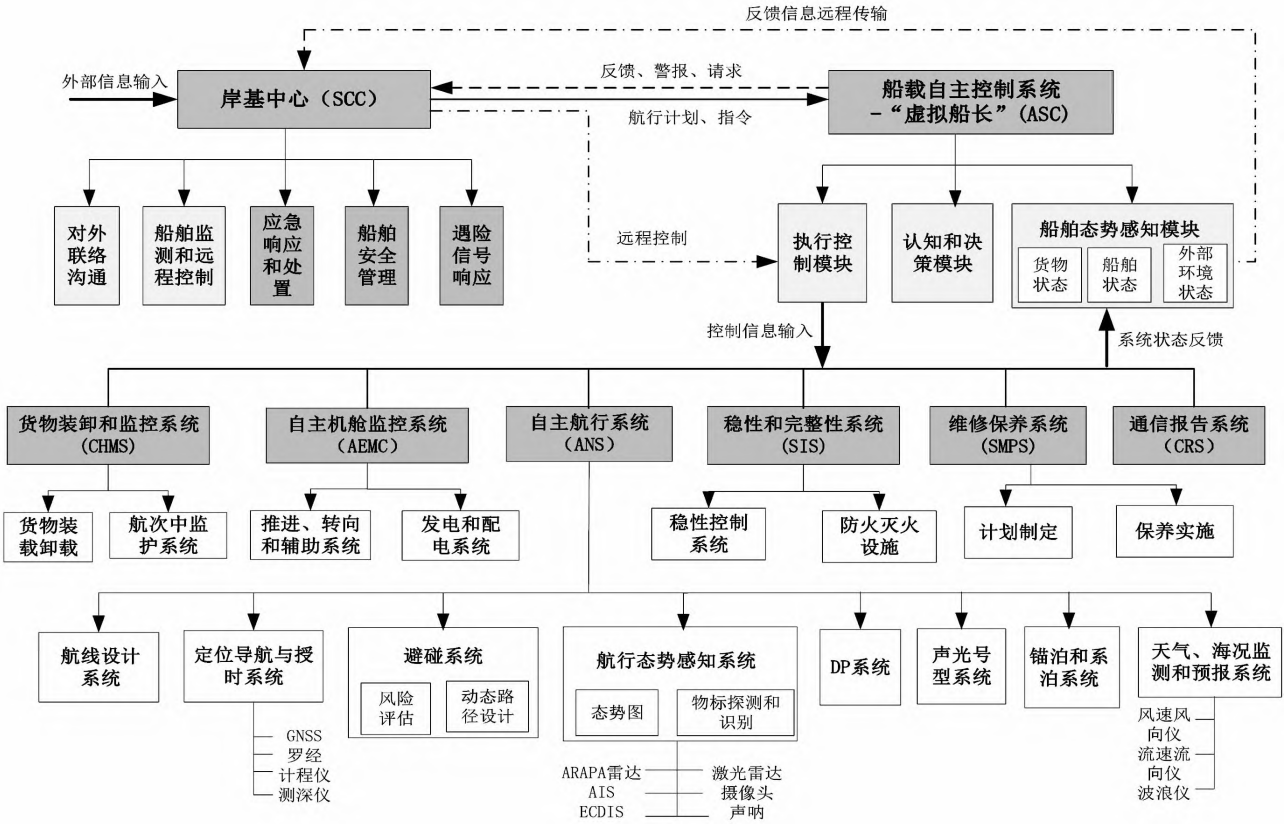

图 2　基于船员功能替代的智能船系统 STAMP 模型

系统分为若干层级,各层级间通过控制回路来实现系统的控制目标。总体来看,智能船包含两个分别以 SCC 和 ASC 为控制枢纽的并行系统,其在 SCC 和 ASC 系统交互和协同下运行,其中 SCC 和 ASC 系统为智能船系统的控制器,负责船舶运营期间的态势感知、认识、决策和控制算法或控制策略的输出。SCC 拥有最高的控制权限,ASC 在得到 SCC 授权或通信中断情况下,可对船舶进行控制。

2.3　不安全行为及损失场景分析

针对船舶航行期间可能出现的风险损失(碰撞、搁浅或失控),结合航行场景中系统边界的界定,可确定系统级危险及约束。以航行过程中船舶与固定或浮动的物标发生碰撞为例,其系统级的危险为未保持安全距离,由此可得出系统级的安全约束为船舶须与固定或浮动的物标保持足够的安全距离。以分析转向与推进器子系统的控制行为–航向与航速控制加以说明分析过程, 超出安全约束的 6 组典型的不安全控制行为(UCAs),记作 UCA–1~ UCA–6,如表 1 所示。

表 1　不安全控制行为的识别

控制行为	未提供	提供了导致的危险	提供得过早、过晚	提供的持续时间过长或过短
航速和航向控制	UCA–1：物标与本船存在碰撞危险时，未提供航向和航速控制。	UCA–2：物标与本船存在碰撞危险时,提供了错误的航向和航速控制。 UCA–3:物标与本船不存在碰撞危险时,提供了错误的航向和航速控制。	UCA–4：物标与本船存在碰撞危险时，航向和航速控制提供过晚。	UCA–5:物标与本船存在碰撞危险时,航向和航速控制停止过早。 UCA–6:物标与本船存在碰撞危险时,航向和航速控制停止过晚。

在识别了系统不安全控制行为(UCA-1~ UCA-6)后,通过对不同航行场景中系统损失的致因场景分析,结合图 2 分层控制结构,可将控制回路映射到具体的物理组件,进一步细化组件间约束关系,可导出引发不安全控制行为的影响因素。如表 2 所示,表中列出了产生不安全控制行为的致因场景以及具体的原因。综合分析具体原因发现,智能船航行期间导致系统不安全控制行为的原因可从 3 个方面归纳,即系统组分失效、外部环境干扰以及系统组分间不安全交互。当出现上述单个或多个原因时,系统控制回路中可能会出现不恰当的控制行为或错误反馈信息,从而导致危险的发生。

表 2 不安全控制行为影响因素的辨识

不安全控制行为	致因场景分析		根本致因归纳
	航行场景 1:自主控制(AC)	航行场景 2:远程控制(RC)	
UCA-1	传感器故障(雷达、ECDIS、GNSS 等),无法监测到物标;控制算法缺陷、导致控制指令丢失;船舶操控设备故障	传感器故障(雷达、ECDIS、GNSS 等);岸基作业人员疏忽、未能发现危险;远程操控设备或船舶操控设备故障	组分失效(感知器/控制器/执行器)
	无法接收反馈信息;未执行控制命令;软件工程师缺乏对最新规则或潜在交通场景的了解	无法接收反馈信息;ASC 与 RCC 之间的合作不力;通信故障或中断;控制指令未被执行	不全交互
	雨、雪因素导致杂波干扰;复杂的交通态势	雨、雪因素导致杂波干扰;复杂的交通态势	外部环境扰动
UCA-2	缺乏最新规则或潜在交通场景知识的软件工程师;收到了错误的感知信息;控制指令被错误执行	疏忽或错误操作、自动化、智能化带来的人的自满情绪; 收到了错误的感知信息、错误警报;ASC 与 RCC 之间的合作不力;	不全交互
UCA-3	ECDIS 信息有误、GNSS 数据丢失;控制算法缺陷、导致控制指令错误	ECDIS 信息有误、GNSS 数据丢失; 人为疏忽或决策错误,控制算法缺陷导致控制动作错误	组分失效(感知器/控制器)
	海流或风的变化;复杂的交通态势	能见度低;大浪或大风;复杂的交通态势	外部环境扰动
UCA-4	控制算法缺陷、决策过程延时	岸基操作人员缺乏经验、决策过程延时;控制算法执行过程延时	组分失效(控制器/执行器)
	通信网络延时;操舵系统响应延迟;信息传输延时	通信网络延时;远程操控响应延迟;信息传输延时	不全交互
	自然条件(水流、风或波浪)和交通条件的变化	自然条件(水流、风或波浪)和交通条件的变化	外部环境扰动
UCA-5	操舵系统或动力系统故障;控制算法缺陷导致指令执行得不充分	远程操控设备或船舶操控设备故障; 岸基操作人员认知局限、决策指令不充分; 控制算法缺陷、导致指令执行得不充分	组分失效(感知器/控制器/执行器)
UCA-6	通信中断;控制指令执行得不充分;收到错误或不充分的传感器信息	通信中断;远程控制指令执行得不充分;收到错误或不充分的反馈信息; 岸基作业人员与其他船舶、港口或海事当局的协调不力	不全交互
	自然条件(水流、风或波浪)和交通态势的变化	自然条件(水流、风或波浪)和交通态势的变化	外部环境扰动

3 智能船航行风险评价指标体系构建

根据图 2 基于船员功能替代的智能船系统 STAMP 模型,聚焦智能船航行功能,结合具体的航行场景,根据自主航行系统和自主机舱监控系统及其子系统的分层控制结构,运用 STPA 方法,可推导出在不同场景下影响船舶航行安全的具体原因,具体分析方法如上文所述。将得到的具体原因进行归纳提炼并结合相关研究成果,从组分失效、外部环境干扰以及不安全交互等三个维度构建出智能船航行风险评价指标体系,如图 3 所示。

系统组分的可靠性和鲁棒性是保障船舶航行安全的基础,也是传统安全分析方法研究的重点。本文将系统组分按照感知系统、控制器(岸基和船基)和执行器等进行细分,归纳出面向具体场景的关键性指标。以感知系统失效为例,它包括自感知设备失效、环境感知设备失效、数据库安全性和系统冗余设计等指标。同时,外部环境扰动的随机性和复杂性依然是航行风险形成的主要诱因,需要密切关注。此外,组分间的不安

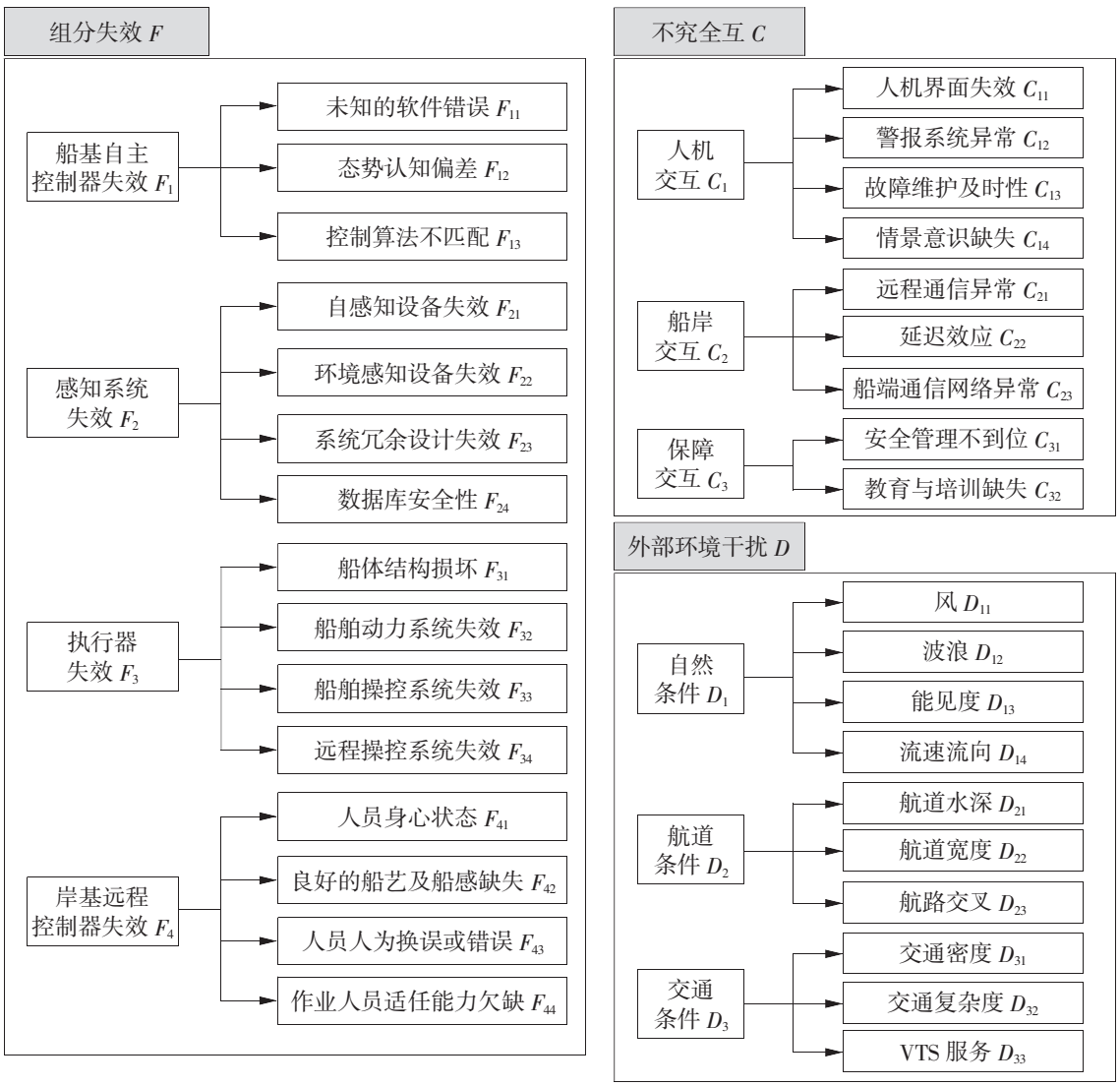

图 3　智能船航行安全风险评价指标体系

全交互也是智能船航行风险控制的重要环节，除面临与普通货船类似的人机交互、人人交互外，船岸远程交互是智能船营运中新的交互方式，稳定的远程通信和船端通信网络是智能船安全航行的先决条件，岸基中心作业人员与船舶空间上的分离，使得时空异构下情景意识缺失、船感缺失等指标同样需要得到重点关注。船舶航行期间通过监测相关评价指标的风险状态，可掌握船舶航行系统总体风险，亦可通过对评价指标实施针对性的安全约束，使之处于良好的状态，以降低风险发生的概率，保障船舶航行安全。

4　结束语

本文构建了基于船员功能替代的智能船航行系统 STAMP 模型，提出智能船航行风险致因 STPA 辨识方法，在此基础上建立智能船航行风险评价指标体系。该指标体系细分到系统或子系统的各个组分，比传统安全指标更加有针对性，所得出的指标不仅涵盖传统意义的人、机、环、管四大类别因素，还包括由技术因素带来的网络安全、感知系统故障、操控系统故障、交互异常等新的风险因素。此方法弥补了传统方法分析复杂系统时对子系统间非线性关联及交互作用难以准确描述的不足，得到的风险因素更加全面、客观。通过对评价指标状态数据的监测，下一步可结合系统工程学及随机过程相关前沿理论，开展系统风险评估或预测研究，为智能船航行风险态势的预测和风险控制措施的实施提供重要依据。

参考文献：

[1]张笛，赵银祥，崔一帆，等.智能船舶的研究现状可视化分析与发展趋势[J].交通信息与安全，2021(1):7-16,34.

[2]LI W, CHEN W, HU S, et al. Risk evolution model of marine traffic via STPA method and MC simulation: A case of MASS along coastal setting [J]. Ocean Engineering, 2023(15):114673.
[3]WRÓBEL K, MONTEWKA J, KUJALA P. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety [J]. Reliability Engineering & System Safety,2017(9):155-169.
[4]RØDSETH Ø J, BURMEISTER H-C. Risk assessment for an unmanned merchant ship[J]. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation,2015(3):357-364.
[5]段尊雷,李玉衡.智能船舶风险分析和对策[J].中国海事,2019(12):15-17.
[6]张文君,张英俊,张闯.基于 HHM-RFRM 理论的智能船舶航行风险识别与筛选[J].安全与环境学报,2023(2):333-340.
[7]周翔宇.面向自主船舶的危险分析方法研究[D].大连:大连海事大学,2020.
[8]ALLISON C K, REVELL K M, SEARS R, et al. Systems theoretic accident model and process (STAMP) safety modelling applied to an aircraft rapid decompression event[J]. Safety Science,2017(10):159-166.
[9]WU C, HUANG L. A new accident causation model based on information flow and its application in Tianjin Port fire and explosion accident [J]. Reliability Engineering & System Safety,2019(2):73-85.
[10]LEVESON N. A new accident model for engineering safer systems [J]. Safety Science,2004(4):237-270.

（责任编辑:张　利）

Construction of Navigation Risk Evaluation Indicator System for Intelligent Vessels Based on STPA Approach

LI Wei[1,2], GUO Yun-long[1], GUO Xing-hua[1], XIA Hong-bing[1]
(1. School of Nautical Technology, Jiangsu Shipping College, Nantong 226010, China;
2. Merchant Marine College, Shanghai Maritime University, Shanghai 201306, China)

Abstract: Aiming at the problem of identifying the risk causes of navigation safety of intelligent ships, based on the STAMP theory, an intelligent ship system model is constructed based on the functional substitution of the crew. Regarding the navigation risk of the ship as a systematic safety control problem, the risk-causing factors are analyzed by applying the STPA method, and then an evaluation index system for the navigation risk of the intelligent ship in constructed on the basis of the three dimensions of the component failures, the interference of the external environment and the insecure interactions. The index system covers a wide range of elements and strongly targets risks, which can scientifically and objectively characterize the safety status of the ship navigation system, and the relevant results have laid a foundation for the subsequent quantitative assessment of the navigation risk of intelligent ships.

Key words: intelligent ship; risk analysis; STAMP; STPA; risk indicators