中文引用格式:席永涛,刘鹏杰,胡甚平,等. 基于STPA和FTPN的海上自主水面船舶航行实时风险评估[J]. 中国安全科学学报,2024,34(8):18-26.

英文引用格式:XI Yongtao,LIU Pengjie,HU Shenping,et al. Real-time risk assessment for maritime autonomous surface ships based on STPA and FTPN[J]. China Safety Science Journal,2024,34(8):18-26.

基于STPA和FTPN的海上自主水面船舶航行实时风险评估*

席永涛[1,2]教授, 刘鹏杰[2], 胡甚平[1]教授, 韩 冰[3]研究员

(1 上海海事大学 商船学院,上海 201306;2 上海海事大学 海洋科学与工程学院,上海 201306;
3 上海船舶运输科学研究所有限公司,上海 200135)

中图分类号:X913.4 **文献标志码**:A **DOI**: 10.16265/j.cnki.issn1003-3033.2024.08.1290

基金项目:水路交通控制全国重点实验室开放课题基金资助(W24CG000042)。

【摘 要】 为实时监测海上自主水面船舶(MASS)航行过程风险,基于系统理论事故模型与过程(STAMP)建立MASS的安全控制结构,采用系统理论过程分析法(STPA)确定损失/事故和系统级危险,识别不安全控制行为并分析损失场景,构建系统状态转化过程模型;采用模糊时间Petri网(FTPN)建模,以设定的MASS航行场景得到相关模糊时间函数并推算FTPN的情态演进;引入新的风险水平表达式并通过系统实时损失/事故二维路径图来可视化系统的实时风险水平和系统不安全状态的转化路径。结果表明:设定的航行场景在当前时刻下,缺少安全水深输入、未更新避碰路径、航向航速不安全、搁浅是风险最高的系统不安全状态,并对应4条风险最高的转化路径;STPA驱动下的FTPN过程模型能全面评估MASS航行的实时风险水平,以系统实时损失/事故二维路径图作为可视化界面,用于监管MASS航行中不安全系统状态并描述其转化路径。

【关键词】 系统理论过程分析(STPA); 模糊时间Petri网(FTPN); 海上自主水面船舶(MASS); 实时风险评估; 转化路径

Real-time risk assessment for maritime autonomous surface ships based on STPA and FTPN

XI Yongtao[1,2], **LIU Pengjie**[2], **HU Shenping**[1], **HAN Bing**[3]

(1 Merchant Marine College, Shanghai Maritime University, Shanghai 201306, China;
2 College of Ocean Science and Engineering, Shanghai Maritime University, Shanghai 201306, China;
3 Shanghai Ship and Shipping Research Institute, Shanghai 200135, China)

Abstract: In order to monitor the risk during the navigation of MASS, the safety control structure of MASS was constructed based on System-theoretic Accident Model and Process (STAMP). STPA was used to define the losses/accidents and system-level hazards, identify unsafe control actions, analyze loss scenarios, and construct an accident model for system state transition. FTPN was used to model the process model, and a given MASS navigation situation was used to obtain the relevant fuzzy time functions and to project the situational evolution of FTPN. A new risk level expression was introduced, and a two-

* 文章编号:1003-3033(2024)08-0018-09; 收稿日期:2024-02-22; 修稿日期:2024-05-25

dimensional path diagram of system loss/accident was used to visualize the real-time system risk level and system unsafe states transition paths. The results show that at the current moment of the set navigation situation, no safe water depth input, no updated collision avoidance path, unsafe heading and speed, and grounding are the highest risk system unsafe states and correspond to the four highest risk transition paths. The study shows that the FTPN process model driven by STPA can comprehensively assess the real-time risk level of MASS navigation. Visualize real-time risk with a two-dimensional path diagram of real-time losses/accidents of the system, which can monitor the unsafe system states during MASS navigation and describe their transition paths.

Keywords: systems-theoretic process analysis (STPA); maritime autonomous surface ships (MASS); fuzzy-timing Petri net (FTPN); transition path; real-time risk assessment

0 引　言

海上自主水面船舶(Maritime Autonomous Surface Ships, MASS)是船舶工业的发展趋势,其自主航行系统基于感知、决策、执行的反馈和控制回路,具备更强的规划和再规划能力[1]。从系统角度来看航行事故的致因,归结为不充分的安全约束,需要在航行过程中加强控制和安全约束[2]。因此,船舶航行风险评估与监测应具有动态性并实施到自主船舶的控制系统中,为船舶提供评估和监管风险的能力并保证系统完整性[1]。

自主船舶系统复杂性高且仍将不断增加,研究表明:系统理论过程分析法(Systems-Theoretic Process Analysis, STPA)在复杂系统安全分析方面更具优势[2],其基于系统理论事故模型与过程(System-Theoretic Accident Modeling and Processes, STAMP),不仅将事故发生归因于组件故障,而且包括系统组件之间的不安全交互[3]。STAMP/STPA 在 MASS 安全研究中呈现 2 种趋势,一是直接应用[4-5];二是与其他方法结合,以实现量化分析[1,6]。但相关研究多集中在风险建模、静态危险识别和分析上。虽有研究采用贝叶斯网络实现了安全水平的动态计算,但由于并非所有故障都具有随机性,如软件故障和人因,因此,使用贝叶斯网络等概率工具计算安全水平并不严格符合 STAMP 的假设[3]。另一方面,STPA 更关注于系统受控过程中的时间、空间和逻辑[7],故 ZELESKIDS 等[7]通过提出 RealTSL 方法来实时确定复杂系统的安全水平,但没有考虑实时系统数据的不确定性和损失/事故路径的潜在组合。

因此,笔者拟基于 STAMP 建立 MASS 的安全控制结构,采用 STPA 确定损失/事故和系统级危险,识别不安全控制行为并分析损失场景,将 STPA 的输出视为可能的不安全系统状态,构建系统状态转化的过程模型,转化为模糊时间 Petri 网(Fuzzy-Timing Petri Net,FTPN);利用该网对系统状态转化中的时态现象进行时间建模和可能性分析;引入新的安全水平表达式来衡量系统在特定时刻的风险水平,以系统实时损失/事故二维路径图作为可视化界面,以期为 MASS 的航行监管和风险控制提供参考。

1 实时风险评估的理论基础

STPA-FTPN 实时风险评估方法的基础是 STPA 危害分析和 FTPN 过程模型。STPA 将系统的安全性问题视作系统的涌现性,其输出是系统不安全状态,并关联事故的可能发生方式[7],这是构建实时风险模型的基础。FTPN 考虑到系统状态转化的时序特性,基于 STPA 的输出构建不安全系统状态转化的过程模型。所提出的实时风险评估方法旨在实时监管系统运行中的不安全状态,使其能够针对最有可能先发生的不安全系统状态做出决策,提早应对以避免事故发生。

STPA-FTPN 实时风险评估方法采用 STAMP 事故模型的定义和假设,其理论依据为:①风险是不确定性对目标的影响[8],并不是所有系统故障都具有随机性[9];②系统接近一个意外状态的程度是动态的[7];③STPA 可全面描述和分析导致事故的不安全系统状态转化[7];④FTPN 可实现系统状态转化的建模[10]。

2 实时风险评估方法

2.1 实时风险评估模型

STPA-FTPN 实时风险评估方法分为 3 个阶段:①系统不安全状态识别,通过 STPA 识别和分析目标系统的危害,获取系统损失/事故、系统级危险、不安全控制行为、损失场景及追溯路径;②系统不安全状态转化模型的构建,基于 STPA 的输出,通过

FTPN 建立目标系统状态转化的过程模型;③系统实时风险评估,通过 FTPN 的完全情态集和新的系统风险水平表达式评估系统的实时风险水平,并以系统实时损失/事故二维路径图作为可视化界面。

STPA-FTPN 方法的阶段、步骤及他们间的相互关系如图 1 所示。STPA-FTPN 实时风险评估过程需要:①STPA 的输出。损失/事故 A、系统级危险 H、不安全控制行为 U、损失场景 L 和追溯路径。②网初始情态。由系统及传感器数据流监测。③模糊延迟。模糊延迟与系统状态转化相关,通过历史数据、试验数据和专家知识获得。④当前系统所处的运行模式。STPA 的每个输出都有其所属的运行模式,系统在不同运行场景其运行模式不同,运行模式由系统运行过程中提供的反馈数据流提供。

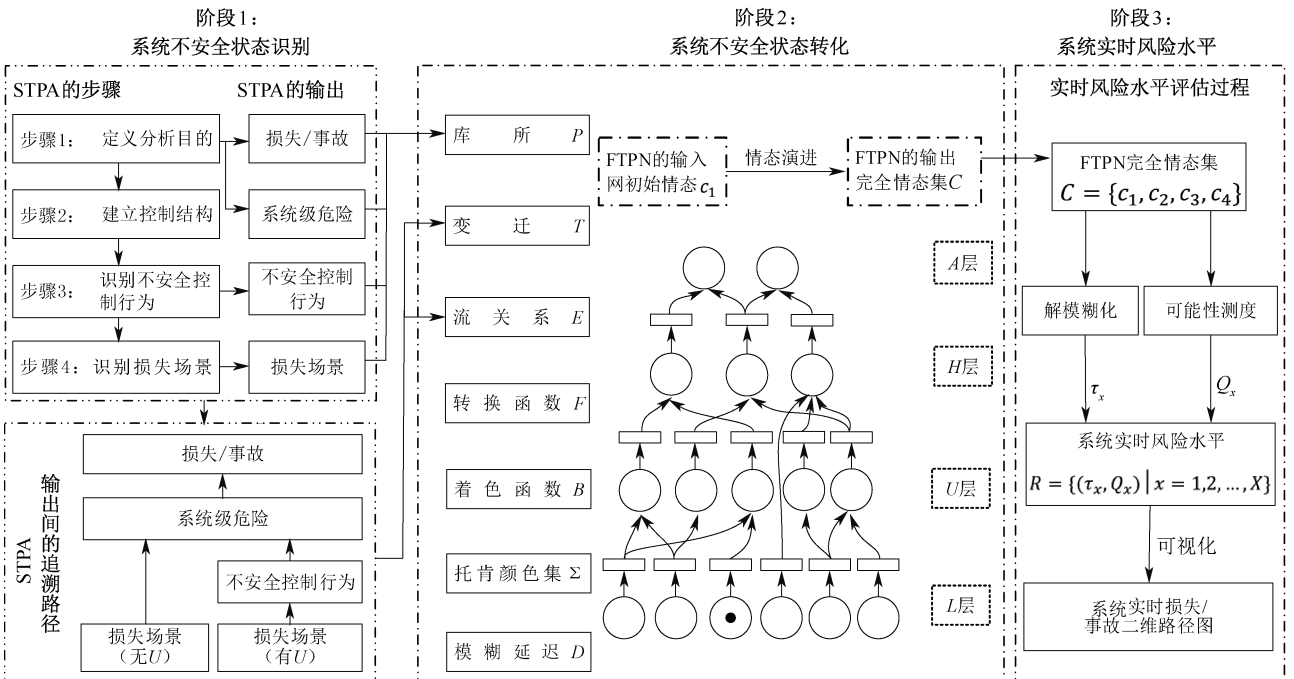

图 1 STPA-FTPN 方法概览

Fig. 1 Overview of STPA-FTPN method

2.2 系统不安全状态识别

第 1 阶段识别和分析系统的不安全状态,定义相应的系统级安全约束并实时监管,确保系统事故不会发生。步骤如下:

1) 定义分析目的。包括定义损失/事故、识别系统级危险、确定系统级安全约束。危险是一种系统状态或一系列条件,在特定的最不利环境下,会导致事故/损失[3]。

2) 建立系统控制结构。控制结构是由反馈控制回路组成的系统模型[3],其通过一套反馈控制回路为系统建模,捕捉功能性关系及相互作用。

3) 识别不安全控制行为。不安全控制行为指特定情境及最坏环境可能导致危险的控制行为[3]。

4) 识别损失场景。损失场景描述的是可能导致不安全控制行为以及危险的诱因[3],识别损失场景即识别系统中可能出现不安全控制的原因并构建合适的情境来解释。

5) 构建追溯路径。追溯路径表示 STPA 输出间相互转化的复杂关系。

2.3 系统不安全状态转化

建立系统不安全状态转化的过程模型,通过监测当前系统的不安全状态,发现其转化路径并实现未来不安全系统状态的预警。

系统不安全状态转化过程模型中的不确定性信息采用可能性理论处理[11]。基于 Petri 网[10]和模糊时间高级 Petri 网(Fuzzy-Timing High Level Petri Nets,FTHN)[12]理论,考虑系统状态转化的时序特性,构建系统不安全状态转化的 FTPN 过程模型。FTPN 为由库所 P、变迁 T、流关系 E、转换函数集 F、托肯颜色集 Σ、着色函数 B 和模糊延迟 D 组成的七元组,即 $N=\{P,T,E,F,\Sigma,B,D\}$。

FTPN 中托肯 t_k/P_i 具备 4 种颜色。托肯所在库所 P_i、生成路径 v、路径完整度 n[7]、模糊时间戳 $\pi_{t_k/P_i}(\tau)$。$t_k/P_i=\{P_i,v,n,\pi_{t_k/P_i}(\tau)\}$ 表示生成路径

为 v 、路径完整度为 n、模糊时间戳为 $\pi_{t_k/P_i}(\tau)$ 的托肯位于库所 P_i ,其中,v 为生成该托肯的库所序列,如 $v = P_S P_U$ 表示生成路径为 $P_S \rightarrow P_U$,P_S 表示输入库所,t 为托肯,i 为系统不安全状态的符号,$k = 1, 2, \cdots, K$,K 为库所 P_i 内托肯的数目。FTPN 过程模型的构建步骤如下:

1) 依据 STPA 输出定义 FTPN 中的库所 P。即系统 4 类不安全状态(A、H、U、L)分别由 FTPN 的 4 个层次库所 P_A、P_H、P_U、P_L 表示。

2) 依据追溯路径确定 FTPN 的变迁 T 和流关系 E ,并定义网的转换函数 F 和算法。T 表示其前集库所向后集库所发生转化的可能条件的集合,除 A 层库所外,每个库所仅对应一个变迁且仅与该变迁存在唯一的流关系 $P \times T$,该变迁与后集库所的多个流关系 $T \times P$ 由其前后集库所间的追溯路径确定。

3) 实时监测系统不安全状态,以托肯 $t_S/P_S = \{P_s, P_s, n, 0\}$ 赋予相应库所 P_s ,得到 FTPN 的初始情态 c_1,其中, $P_s = \{P_A, P_H, P_U, P_L\}$,$n = \{1,2,3,4\}$。

4) 计算网可达路径上的模糊延迟 D。

5) 将 FTPN 转化为系统状态转化的过程模型。

2.4　系统的实时风险水平测量

系统不安全状态转化过程模型中,系统实时风险水平评估需考虑 3 个关键参数:系统不安全状态发生前的剩余时间 τ 、路径完整度 n 和状态转化最先发生的可能性 Q。其中:

1) 系统不安全状态发生前的剩余时间 τ。τ 是对 RealTSL 方法中事故发生前的剩余时间的扩展。τ 表示当前系统不安全状态遵循追溯路径抵达未来系统不安全状态的剩余时间。τ 越小,系统不安全状态风险越高。

2) 路径完整度 n。n 表示系统不安全状态转化过程模型中可能发生的不安全状态接近 A 层库所的程度。其值($n = \{1,2,3,4\}$)越大,即越接近损失/事故,不安全状态风险越高。

3) 状态转化最先发生的可能性 Q。Q 表示相同路径完整度的系统不安全状态最先向更高路径完整度系统不安全状态转化的可能性。Q 越大,则系统不安全状态的风险越高。

因而系统实时风险可根据该时刻下 FTPN 完全情态集 $C = \{c_1, c_2, c_3, c_4\}$ 内的托肯来计算,其中,c_1、c_2、c_3、c_4 为网的 4 种情态。系统风险水平以集合 $R = \{(\tau_x, Q_x) \mid x = 1,2,\cdots,X\}$ 表示,其中,X 为完全情态集 C 下全部托肯的数目,τ_x 为完全情态集 C 内各托肯模糊时间戳解模糊化所得的精确时刻值,表示距离未来可能的系统不安全状态的剩余时间。Q_x 为托肯相较于相等路径完整度的其他托肯最先发生的可能性测度值。

为得到 FTPN 的完全情态集 C,需要采用模糊时间戳 $\pi_{t_k/P_i}(\tau)$ 和模糊延迟 $d_{E,v}(\tau)$ 2 个模糊时间函数对系统状态转化中的时态现象建模,演进 FTPN 的情态并进行可能性分析。

1) $\pi_{t_k/P_i}(\tau)$ 。托肯的模糊时间戳是该托肯抵达 P_i 时间 τ 的可能性数值估计,即模糊时间函数。

2) $d_{E,v}(\tau)$ 。模糊延迟是与流关系 E 和托肯颜色 v 相关的模糊时间函数,表示托肯从发生变迁到变迁完成(状态转化完成)的模糊时间延迟。

其中,模糊时间函数是从时间尺度到真实区间 $[0,1]$ 的函数,表示时间或时间点 τ 的可能性的程度,并采用梯形或三角形分布,用参数 $p(a_1, a_2, a_3, a_4)$ 来表示,其中, p 为系统状态转化时间的隶属度,其值域为 $[0,1]$ 。在特定的最不利环境下,$[a_2, a_3]$ 表示状态转化确定发生的时间区间,$[a_1, a_2]$ 和 $[a_3, a_4]$ 表示状态转化可能发生的时间区间,$[a_1, a_4]$ 之外的区间表示状态转化肯定不发生的时间区间。

模糊时间区间 $\pi_a(\tau) = p_a(a_1, a_2, a_3, a_4)$ 和 $\pi_b(\tau) = p_b(b_1, b_2, b_3, b_4)$ 的运算:交集 min、并集 max、加法⊕见下式。

$$\pi_a(\tau) \cap \pi_b(\tau) = \min\{\pi_a(\tau), \pi_b(\tau)\} \quad (1)$$

$$\pi_a(\tau) \cup \pi_b(\tau) = \max\{\pi_a(\tau), \pi_b(\tau)\} \quad (2)$$

$$\pi_a(\tau) \oplus \pi_b(\tau) = \min\{p_a, p_b\} (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4) \quad (3)$$

基于上述定义和算法,情态演进依据 FTPN 的 4 个层次演进,具体步骤如下:

1) 确定网的初始情态 c_1。c_1 依靠传感器数据流和系统本身监测得到, c_1 中所有输入库所内的托肯 $t_S/P_S = \{P_s, P_s, n, \pi_{t_S/P_S}(\tau)\}$,其中, $\pi_{t_S/P_S}(\tau)$ 为输入库所内托肯的模糊时间戳,且 $\pi_{t_S/P_S}(\tau) = (0,0,0,0)$,$P_S$ 为输入库所集中的一个库所, $n = \{1,2,3,4\}$,文中以 $n = 1$、$P_s = P_L$ 为例。

2) 搜索输入库所与 A 层库所间的可达路径。

3)计算后集库所内托肯 t_k/P_U 的模糊时间戳 $\pi_{t_k/P_U}(\tau)$:$\pi_{t_k/P_U}(\tau) = \pi_{t_1/P_L}(\tau) \oplus d_{E,v}(\tau)$,则 $t_k/P_U = \{P_{U_Y}, P_L P_{U_Y}, 2, \pi_{t_k/P_U}(\tau)\}$ 。其中,Y 为以 P_L 为输入库所的可达路径中 U 层库所的数目,U 层托肯生成

完毕后得到网的情态 c_2。

4) FTPN 中 4 个层次自下而上类推,直至得到完全情态集 C。

得到系统该时刻的完全情态集后,为获取精确的时间信息 τ_x,需要对模糊时间戳解模糊化,计算见下式。而某一状态转化最先发生的可能性 Q_x 采用模糊时间区间不等式[13]计算。

$$\tau_x = \mathrm{d}\pi(\tau) = \frac{\int \tau\pi(\tau)\,\mathrm{d}\tau}{\int \pi(\tau)\,\mathrm{d}\tau} \tag{4}$$

通过解模糊化和可能性测度,得到系统不安全状态发生时刻的精确值 τ_x 和转化最先发生的可能性测度 Q_x,以集合 $R = \{(\tau_x, Q_x) \mid x = 1,2,\cdots,X\}$ 来表示当前时刻系统的风险水平,并以系统实时损失/事故二维路径图作为可视化界面。

3 实时评估方法的实例应用

3.1 MASS 航行场景设定

自主船舶避碰场景及过程如图 2 所示,图中,沿海自主航行集装箱船 S_1,S_1 由岸基控制中心(Shore-based Control Centre,SCC)的操作员监督,在紧急情况或执行复杂任务时进行干预。S_1 船的自主等级为 Lloyd's Register 自主等级中的 AL4[14],即控制人员监督决策执行并有权干预、监督所有决策和行动的自主执行、有权干预高影响力决策。设定的会遇场景和相关船舶基本信息如图 2 所示。

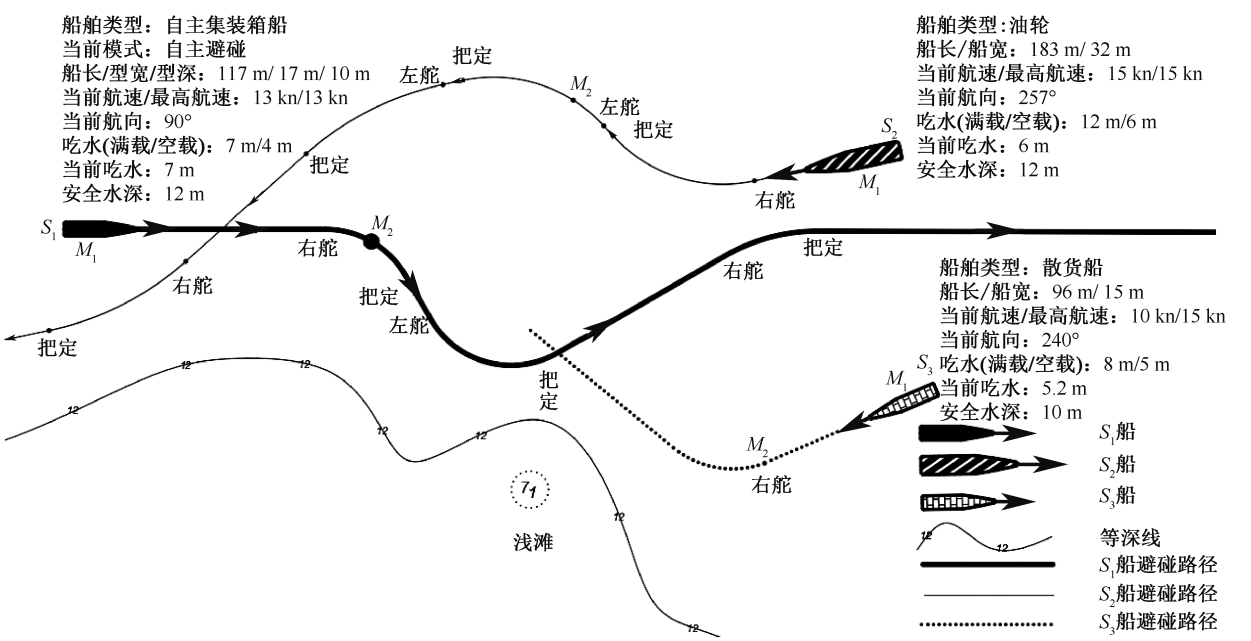

图 2 自主船舶避碰场景及过程

Fig. 2 MASS collision avoidance situations and process

研究关注 M_2($M_2 = M_1 + 415$ s)时刻,M_1 为当前所处时刻,其中,S_1 船为自主集装箱船,S_2 船为油轮,S_3 船为散货船。M_1 时刻,S_2 船在 S_1 船左舷 5°,距离约 4.1 n mile 处,S_1 船与 S_2 船航向相交并构成对遇局面,若 2 船保向保速,最小会遇距离(Distance Closest Point of Approach,DCPA)约为 410 m,最短会遇时间(Time Closest Point of Approach,TCPA)约为 545 s,将构成碰撞危险。且 S_1 船右舷 31° 约 2.7 n mile 处存在浅滩,右舷 12°约 4.4 n mile 处 S_3 船正以 247°航向航行。因此,按照现行《1972 年国际海上避碰规则》,S_1 船自主避碰系统在 M_1 时刻提供的避碰路径如图 2 中粗有向实线所示,S_2 船和 S_3 船的实际避碰路径分别如图 2 所示有向细实线和虚线所示。

3.2 系统危害识别与分析

S_1 船航行中的系统级事故中,仅考虑"A_1:S_1 船发生碰撞"和"A_2:S_1 船发生搁浅";且只考虑系统组件间不安全交互和组件故障,而不考虑不充分的控制算法或过程模型和海况/风况。

船舶碰撞经过 4 个阶段:无碰撞风险(No Collision Risk,NCR)、有碰撞风险(Risk of Collision,CR)、紧迫局面(Close-quarter Situation,CS)和紧迫危险(Immediate Danger,ID)[15]。4 个阶段的界定可作为定义系统级危险及其安全约束的参考,以定义

和计算相关模糊时间函数。判断碰撞危险的主要依据是 DCPA/TCPA,依据 IMO 的 DCPA 和 TCPA 规定(2 船距离非常接近,DCPA≥0.5 n mile;当 2 船航向相交时,TCPA≥6 min)。CR 和 CS 的界定为 2 船能否凭借单船行动在安全距离(1 n mile)上驶过。CS 和 ID 的界定为 2 船能否凭借单船行动避免碰撞,此距离为 0.2 n mile。将船舶凭借自身行动已无法避免搁浅定义为搁浅系统级危险之一,此距离为 0.2 n mile。

第 1 步:定义分析目的。其输出见表 1。

表 1　STPA 第 1 步:定义分析目的的结果

Table 1　Results of defining the purpose of the analysis

H	库所	系统级危险	安全约束	追溯路径
H_1	P_{H_1}	MASS 未与他船保持安全距离	MASS 需保证不会导致 CS 的安全距离	A_1
H_2	P_{H_2}	MASS 相对他船航向和航速不安全	MASS 需确保当前航向/航速不会导致 CS	A_1
H_3	P_{H_3}	MASS 未满足富余水深限制	MASS 需确保富余水深满足富余水深限制	A_2
H_4	P_{H_4}	MASS 相对浅滩的航向/航速不安全	MASS 需确保当前航向/航速可凭自身行动避免搁浅	A_2

第 2 步:建立系统安全控制结构。参考目前国内外研究[4-5]提出的 MASS 安全控制结构,结合现有实船 YARA BIRKELAND 和智飞号,提出 MASS 的安全控制结构如图 3 所示。

第 3 步:识别不安全控制行为。研究关注自主避碰/航线跟踪系统根据实时数据更新船舶的避碰路径。因根据实时数据提供避碰路径是离散控制行为,不存在提供避碰路径持续太久或停止过早这类不安全控制行为。识别出的不安全控制行为有 4 个:① U_1:自主避碰/航线跟踪系统未提供避碰路径更新;② U_2:自主避碰/航线跟踪系统提供了安全的避碰路径更新,但自主船舶没有正确遵循;③ U_3:自主避碰/航线跟踪系统提供了不安全的避碰路径更新;④ U_4:自主避碰/航线跟踪系统未及时提供避碰路径更新。

第 4 步:识别损失场景。U_1、U_2、U_3、U_4 所识别出的损失场景总计 35 个。

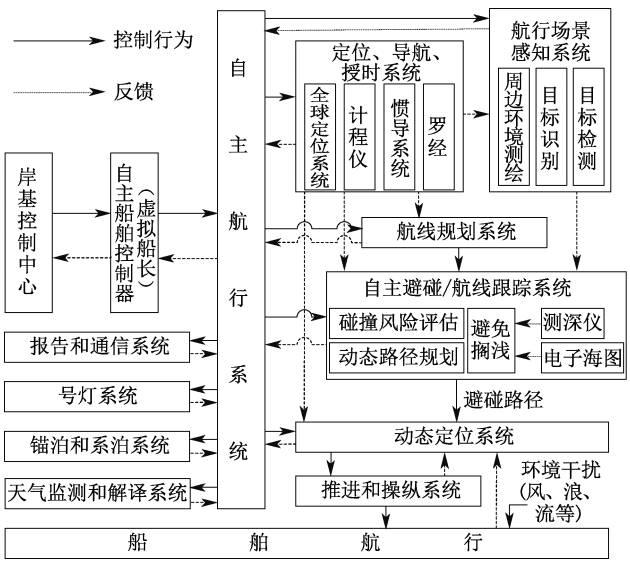

图 3　MASS 的安全控制结构

Fig. 3　Safety control structure of MASS

第 5 步:构建追溯路径并与 FTPN 对应。该步骤输出见表 2。

表 2　STPA 输出间的追溯路径及对应的 FTPN 库所

Table 2　Traceability between the outputs of STPA and the corresponding FTPN places

STPA 输出	追溯路径			
A	$A_1\backslash P_{A_1}$		$A_2\backslash P_{A_2}$	
H	$H_1\backslash P_{H_1}$	$H_2\backslash P_{H_2}$	$H_3\backslash P_{H_3}$	$H_4\backslash P_{H_4}$
U	$U_1\backslash P_{U_1}$; $U_2\backslash P_{U_2}$; $U_3\backslash P_{U_3}$; $U_4\backslash P_{U_4}$			
L	$U_1\backslash P_{U_1}\leftarrow$ $L_1\backslash P_{L_1}$ - $L_{11}\backslash P_{L_{11}}$	$U_2\backslash P_{U_2}\leftarrow$ $L_{12}\backslash P_{L_{12}}$ - $L_{15}\backslash P_{L_{15}}$	$U_3\backslash P_{U_3}\leftarrow$ $L_{16}\backslash P_{L_{16}}$ - $L_{24}\backslash P_{L_{24}}$	$U_4\backslash P_{U_4}\leftarrow$ $L_{25}\backslash P_{L_{25}}$ - $L_{35}\backslash P_{L_{35}}$

注:$A_1\backslash P_{A_1}$ 表示 STPA 的输出 A_1 与 FTPN 的库所 P_{A_1} 对应;$U_1\backslash P_{U_1}\leftarrow L_1\backslash P_{L_1}$-$L_{11}\backslash P_{L_{11}}$ 表示 L_1—L_{11} 均与 U_1 存在追溯路径。

3.3　构建 FTPN 过程模型

STPA 输出间的追溯路径描述的是系统不安全状态的转化,并最终导致事故发生的可能场景。基于 STPA 输出间的追溯路径所构建的 FTPN 过程模型如图 4 所示。

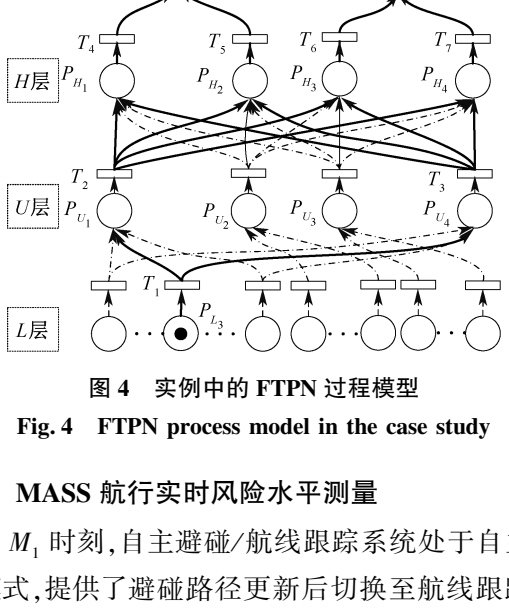

图 4　实例中的 FTPN 过程模型

Fig. 4　FTPN process model in the case study

3.4　MASS 航行实时风险水平测量

M_1 时刻,自主避碰/航线跟踪系统处于自主避碰模式,提供了避碰路径更新后切换至航线跟踪模式, M_2 时刻 S_3 船右舵让路,S_1 船需更新避碰路径,而自主航行系统未提供避碰路径更新必要的安全水深,即表示 FTPN 中,损失场景层库所 P_{L_3}:自主航行系统未提供避碰路径更新必要的控制输入(如 CPA 和 TCPA、安全水深、船舶安全域)。具备托肯 $t_1/P_{L_3}=\{P_{L_3},P_{L_3},1,(0,0,0,0)\}$。

变迁点火代表系统不安全状态的转化,因而变迁表示系统不安全状态转化的可能条件集, T_1— T_7 的具体含义见表 3。

表 3　实例中变迁的含义

Table 3　Description of the transitions in the case study

T	含义
T_1	SCC 未得到高风险警报、未提供必要的控制输入等
T_2	自主避碰/航线跟踪系统未提供避碰路径更新
T_3	S_1 船已处于紧迫危险阶段或已无法避免搁浅
T_4	S_1 船未减速停止、警告他船等
T_5	S_1 船未紧急改变航向航速、警告他船等
T_6	S_1 船未减速停船、改变船体姿态、减少吃水等
T_7	S_1 船未紧急改变航向航速等

以时间为关键参数之一的航行场景中,航速是影响时间的主要参数之一,影响航速的因素有通航环境、通航秩序、海洋气象及船舶操纵性能等[16]。航速的不确定性会导致时间的不确定性。系统不安全状态转化过程中,采用模糊时间函数描述时间的不确定性, a_1 和 a_4 分别表示以可能的最高、最低速度计算获得的时间, $a_2=a_3$ 表示考虑可能的航速变化获得的时间。故基于实时数据和建立的数据集,得到相关模糊时间函数 $d_{E,v}(\tau)$ 见表 4。M_2 时刻,FTPN 过程模型如图 4 所示,其中,粗实线有向弧表示可能导致事故的系统不安全状态转化路径,即可达路径。情态演进和计算后得到 M_2 时刻 FTPN 的完全情态集,见表 5。

表 4　相关模糊延迟 $d_{E,v}(\tau)$

Table 4　Relevant fuzzy time function $d_{E,v}(\tau)$

E	v	$d_{E,v}(\tau)$	E	v	$d_{E,v}(\tau)$
$T_1\times P_{U_1}$	P_{L_3}	$d_1(\tau)=(177,190,190,207)$	$T_1\times P_{U_4}$	P_{L_3}	$d_{10}(\tau)=(390,449,449,564)$
$T_2\times P_{H_1}$	$P_{L_3}P_{U_1}$	$d_2(\tau)=(113,120,120,132)$	$T_3\times P_{H_1}$	$P_{L_3}P_{U_4}$	$d_{11}(\tau)=(0,0,0,0)$
$T_4\times P_{A_1}$	$P_{L_3}P_{U_1}P_{H_1}$	$d_3(\tau)=(192,213,213,216)$	$T_4\times P_{A_1}$	$P_{L_3}P_{U_4}P_{H_1}$	$d_{12}(\tau)=\infty$
$T_2\times P_{H_2}$	$P_{L_3}P_{U_1}$	$d_4(\tau)=(167,188,188,211)$	$T_3\times P_{H_2}$	$P_{L_3}P_{U_4}$	$d_{13}(\tau)=\infty$
$T_5\times P_{A_1}$	$P_{L_3}P_{U_1}P_{H_2}$	$d_5(\tau)=(139,145,145,157)$	$T_5\times P_{A_1}$	$P_{L_3}P_{U_4}P_{H_2}$	$d_{14}(\tau)=\infty$
$T_2\times P_{H_3}$	$P_{L_3}P_{U_1}$	$d_6(\tau)=(267,278,278,356)$	$T_3\times P_{H_3}$	$P_{L_3}P_{U_4}$	$d_{15}(\tau)=(14,14,14,14)$
$T_6\times P_{A_2}$	$P_{L_3}P_{U_1}P_{H_3}$	$d_7(\tau)=(28,28,28,28)$	$T_6\times P_{A_2}$	$P_{L_3}P_{U_4}P_{H_3}$	$d_{16}(\tau)=(14,14,14,14)$
$T_2\times P_{H_4}$	$P_{L_3}P_{U_1}$	$d_8(\tau)=(0,0,0,0)$	$T_3\times P_{H_4}$	$P_{L_3}P_{U_4}$	$d_{17}(\tau)=(0,0,0,0)$
$T_7\times P_{A_2}$	$P_{L_3}P_{U_1}P_{H_4}$	$d_9(\tau)=(274,306,306,396)$	$T_7\times P_{A_2}$	$P_{L_3}P_{U_4}P_{H_4}$	$d_{18}(\tau)=(28,28,28,28)$

根据完全情态集 $C=\{c_1,c_2,c_3,c_4\}$ 将 $R=\{(\tau_x,Q_x)\mid x=1,2,\cdots,X\}$ 依据路径完整度的不同绘制在二维坐标系中,可得到完整的系统实时损失/事故二维路径图(图 5)。其中,纵轴为系统不安全状态发生前的剩余时间 τ,横轴为托肯的路径完整度 n,并且系统状态转化最先发生的可能性以渐变色表示,颜色越深即可能性越高。

在当前时刻和环境下的系统损失/事故二维路径图中,风险最高的系统状态及转化路径被直观表达,同渐变色区域内越靠近左下角的托肯所代表的系统不安全状态风险越高,意味着在同渐变色区域内,所代表的系统不安全状态最可能先发生。S_1 船在 M_2 时刻,各层中风险最高的不安全系统状态分别为 L_3、U_1、H_4、A_2,托肯 $t_2/P_{A_2}=\{P_{A_2},P_{L_3}P_{U_4}P_{H_4}P_{A_2},$

表 5　实例研究 FTPN 情态演进和计算结果

Table 5　Case evolution and calculation results of FTPN in the case study

情态	层	库所	托肯	托肯颜色	(τ_x, Q_x)
c_1	L 层	P_{L_3}	t_1/P_{L_3}	$\{P_{L_3}, P_{L_3}, 1, (0,0,0,0)\}$	(0,1)
c_2	U 层	P_{U_1}	t_1/P_{U_1}	$\{P_{U_1}, P_{L_3}P_{U_1}, 2, (177,190,190,207)\}$	(191,1)
		P_{U_4}	t_1/P_{U_4}	$\{P_{U_4}, P_{L_3}P_{U_4}>, 2, (390,449,449,564)\}$	(468,0)
c_3	H 层	P_{H_1}	t_1/P_{H_1}	$\{P_{H_1}, P_{L_3}P_{U_1}P_{H_1}, 3, (290,310,310,339)\}$	(313,0)
			t_2/P_{H_1}	$\{P_{H_1}, P_{L_3}P_{U_4}P_{H_1}, 3, (390,449,449,564)\}$	(468,0)
		P_{H_2}	t_1/P_{H_2}	$\{P_{H_2}, P_{L_3}P_{U_1}P_{H_2}, 3, (344,378,378,418)\}$	(380,0)
			t_2/P_{H_2}	$\{P_{H_2}, P_{L_3}P_{U_4}P_{H_2}, 3, \infty\}$	$(\infty, 0)$
		P_{H_3}	t_1/P_{H_3}	$\{P_{H_3}, P_{L_3}P_{U_1}P_{H_3}, 3, (444,468,468,563)\}$	(492,0)
			t_2/P_{H_3}	$\{P_{H_3}, P_{L_3}P_{U_4}P_{H_3}, 3, (404,463,463,578)\}$	(482,0)
		P_{H_4}	t_1/P_{H_4}	$\{P_{H_4}, P_{L_3}P_{U_1}P_{H_4}, 3, (177,190,190,207)\}$	(191,1)
			t_2/P_{H_4}	$\{P_{H_4}, P_{L_3}P_{U_4}P_{H_4}, 3, (390,449,449,564)\}$	(468,0)
c_4	A 层	P_{A_1}	t_1/P_{A_1}	$\{P_{A_1}, P_{L_3}P_{U_1}P_{H_2}P_{A_1}, 4, (482,523,523,555)\}$	(520,0.348)
			t_2/P_{A_1}	$\{P_{A_1}, P_{L_3}P_{U_1}P_{H2}P_{A_1}, 4, \infty\}$	$(\infty, 0)$
			t_3/P_{A_1}	$\{P_{A_1}, P_{L_3}P_{U_4}P_{H_2}P_{A_1}, 4, (483,523,523,575)\}$	(527,0.445)
			t_4/P_{A_1}	$\{P_{A_1}, P_{L_3}P_{U_4}P_{H2}P_{A_1}, 4, \infty\}$	$(\infty, 0)$
		P_{A_2}	t_1/P_{A_2}	$\{P_{A_2}, P_{L_3}P_{U_1}P_{H_3}P_{A_2}, 4, (472,496,496,591)\}$	(520,0.566)
			t_2/P_{A_2}	$\{P_{A_2}, P_{L_3}P_{U_1}P_{H_3}P_{A_2}, 4, (418,477,477,592)\}$	(496,0.828)
			t_3/P_{A_2}	$\{P_{A_2}, P_{L_3}P_{U_4}P_{H_4}P_{A_2}, 4, (451,496,496,603)\}$	(517,0.779)
			t_4/P_{A_2}	$\{P_{A_2}, P_{L_3}P_{U_4}P_{H_4}P_{A_2}, 4, (418,477,477,592)\}$	(496,0.828)

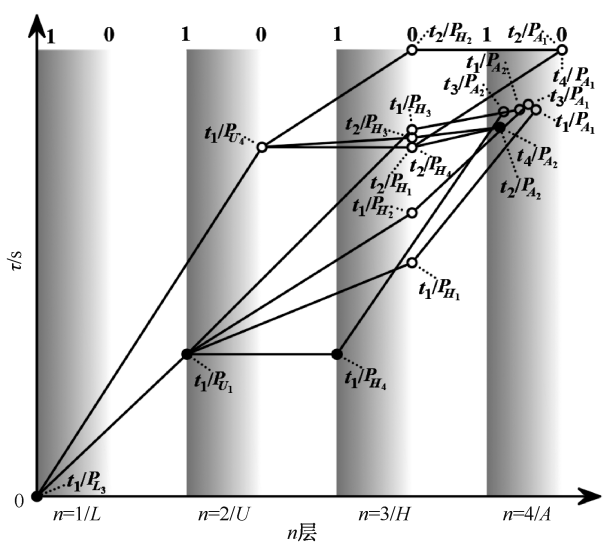

图 5　M_2 时刻下,系统损失 / 事故二维路径图

Fig. 5　Two-dimensional path diagramof the losses or accidents at the moment of M_2

4,(418,477,477,592)} 表示在当前时刻和场景下 A_2 最可能先发生,且转化路径为 $P_{L_3} \rightarrow P_{U_4} \rightarrow P_{H_4} \rightarrow P_{A_2}$。基于此,SCC 应当优先及时确保安全的航向和航速,并尽早提供安全的避碰路径。值得注意的是,最可能以最短时间导致 A_2 发生的不安全控制行为为 U_4,而不是最可能发生的 U_1,即 U_4 导致事故发生的潜力更大。这表明实时风险评估方法中风险最高的损失/事故路径并不是较短路径时序上的延伸,体现了该方法局部最优不是全局最优的思想,可避免紧迫程度更高的潜在损失/事故路径被忽视。

4　结　论

1) 提出的 STPA-FTPN 方法可构建系统不安全状态转化的过程模型,将时间作为关键参数可衡量复杂系统在特定时刻和环境下的系统风险,是量化 STPA 定性分析结果的尝试。

2) 提出的系统风险水平表达式和系统实时损失/事故二维路径图可为实时监管系统风险提供依据。安全管理者可参考系统实时风险准确快速做出反应和决策,以避免损失/事故发生。

3）STPA-FTPN 方法适用于碰撞、搁浅等具有明显时间序列特性的实时风险评估，对火灾等损失/事故适用性不足，受制于 MASS 研究和应用现状，尚未开展验证。

参 考 文 献

[1] UTNE I B, ROKSETH B, SØRENSEN A J, et al. Towards supervisory risk control of autonomous ships[J]. Reliability Engineering & System Safety, 2020, 196: DOI: 10.1016/j.ress.2019.106757.

[2] ZHANG Yingyu, DONG Chuntong, GUO Weiqun, et al. Systems theoretic accident model and process (STAMP): a literature review[J]. Safety Science, 2021: DOI: 10.1016/j.ssci.2021.105596.

[3] LEVESON N G, THOMAS J. STPA handbook[Z]. Massachusetts Institute of Technology, 2018.

[4] 张浦哲, 吴兵, 严新平, 等. 内河船舶远程驾驶控制系统安全分析[J]. 中国安全科学学报, 2022, 32(8): 126-132.
ZHANG Puzhe, WU Bing, YAN Xinping, et al. Safety analysis for remote control system of inland ships [J]. China Safety Science Journal, 2022, 32(8): 126-132.

[5] CHAAL M, VALDEZ BANDA O A, GLOMSRUD J A, et al. A framework to model the STPA hierarchical control structure of an autonomous ship[J]. Safety Science, 2020, 132: DOI: 10.1016/j.ssci.2020.104939.

[6] CEYLAN B O, AKYUZ E, ARSLANOĞLU Y. Modified quantitative systems theoretic accident model and processes (STAMP) analysis: a catastrophic ship engine failure case[J]. Ocean Engineering, 2022, 253: DOI: 10.1016/j.oceaneng.2022.111187.

[7] ZELESKIDIS A, DOKAS I M, PAPADOPOULOS B K. Knowing the safety level of a system in real-time: an extended mathematical model of the STAMP-based RealTSL methodology[J]. Safety Science, 2022, 152: DOI: 10.1016/j.ssci.2022.105739.

[8] RASTRABANK N. Risk management guidelines for banks and financial institutions[R]. Bank of Tanzania, 2018.

[9] 席永涛, 张靓, 付姗姗, 等. 基于 SFN-SD 的北极冰区船舶航行风险传递路径研究[J]. 中国安全科学学报, 2023, 33(4): 52-60.
XI Yongtao, ZHANG Liang, FU Shanshan, et al. Research on risk transfer path of ship navigation in Arctic waters based on SFN and SD [J]. China Safety Science Journal, 2023, 33(4): 52-60.

[10] 吴哲辉. Petri 网导论[M]. 北京: 机械工业出版社, 2006: 1-24.

[11] 杜彦华, 范玉顺. 资源约束下多过程的不确定时间建模与分析[J]. 机械工程学报, 2010, 46(4): 169-176.
DU Yanhua, FAN Yushun. Modeling and analyzing of uncertain time for multi-process of workflows with resource constraints [J]. Journal of Mechanical Engineering, 2010, 46(4): 169-176.

[12] MURATA T. Temporal uncertainty and fuzzy-timing high-level Petri nets[C]. International Conference on Application and Theory of Petri Nets, 1996: 11-28.

[13] ZHOU YI, MURATA T. Petri net model with fuzzy timing and fuzzy-metric temporal logic[J]. International Journal of Intelligent Systems, 1999, 14(8): 719-745.

[14] 周翔宇, 吴兆麟, 王凤武, 等. 自主船舶的定义及其自主水平的界定[J]. 交通运输工程学报, 2019, 19(6): 149-162.
ZHOU Xiangyu, WU Zhaolin, WANG Fengwu, et al. Definition of autonomous ship and its autonomy level[J]. Journal of Traffic and Transportation Engineering, 2019, 19(6): 149-162.

[15] ZHU Qinghua, XI Yongtao, HU Shenping, et al. Spatial-temporal analysis method of ship traffic accidents involving data field: an evidence from risk evolution of ship collision[J]. Ocean Engineering, 2023, 276: DOI: 10.1016/j.oceaneng.2023.114191.

[16] 王胜正, 申心泉, 赵建森, 等. 基于 ASAE 深度学习预测海洋气象对船舶航速的影响[J]. 交通运输工程学报, 2018, 18(2): 139-147.
WANG Shengzheng, SHEN Xinquan, ZHAO Jiansen, et al. Prediction of marine meteorological effect on ship speed based on ASAE deep learning[J]. Journal of Traffic and Transportation Engineering, 2018, 18(2): 139-147.

作者简介： 席永涛 (1977—)，男，河北无极人，博士，教授，博士生导师，主要从事交通运输安全与管理、人因可靠性分析、风险建模与评估方面的研究。E-mail：xiyt@ shmtu.edu.cn。