石油科学通报
Petroleum Science Bulletin

基于 STAMP—STPA 的 LNG 储备库典型事故正演模型构建

胡瑾秋[1*]，董绍华[1]，王融涵[1]，张曦月[1]

中国石油大学(北京)安全与海洋工程学院，北京 102249
* 通信作者, hujq@cup.edu.cn.

收稿日期: 2020−06−25
国家重点研发计划(2017YFC0805801) 和北京市科技新星计划(Z181100006218048) 联合资助

摘要　在相关事故概率统计数据缺少的情况下，为提高LNG储备库的整体安全性，解决传统安全性分析方法无法考虑复杂系统内部关联性、事故分析思路较为分散、忽视组件交互及宏观控制的问题，保证液化天然气储备库分层翻滚事故和火灾事故正演结果的准确性，建立基于系统论事故分析模型(Systems-Theoretic Accident Modeling and Process，STAMP)及系统理论过程分析(System-Theoretic Process Analysis，STPA)的LNG储备库典型事故正演模型，使得后续系统隐患分析、事故原因分析的更加全面完善。首先，根据LNG储罐分层翻滚事故和火灾事故过程中涉及的设备设施、工艺流程及相互间的关联关系，对事故进行初步危险分析、辨识导致事故发生的各个因素、找出危险的关键节点，并在此基础上分析事故所在系统的安全需求及对应的安全性约束，包括可能导致事故发生的控制与反馈操作，建立STAMP模型，模型需包含相关设施、组件之间的控制、反馈关系，和控制反馈回路；然后，采用STPA方法识别LNG保障过程中的四种不安全的控制行为(未提供的控制行为、提供错误或不安全供控制行为、未及时提供控制行为、控制行为结束过早)，并从控制行为执行不充分、反馈信息错误或不足两方面分析事故整体过程中涉及到的初始值(如储罐LTD参数)、当前状态(如进液操作)以及状态转换(如储罐与冷却完成准备进液)，找出导致不安全控制行为的关键原因，建立完整的LNG储备库典型事故正演模型；最后，结合具体事故案例验证分析LNG储备库典型事故正演模型的有效性与可实施性，并将分析结果可视化，以知识图谱的方式直观展现。研究表明：该模型可从控制和约束角度对复杂系统LNG储备库典型事故进行过程分析，使得事故演化过程更加直观、准确，原因梳理更加清晰；从系统的角度考虑了各风险因素在分层翻滚事故和火灾事故正演中的因果关系，为后续LNG储备库的安全管理工作提供了可行、有针对性的价值信息。

关键词　LNG储备库；不安全行为；STAMP—STPA；火灾事故；分层翻滚事故

STAMP-STPA based forward model construction of typical LNG repository accidents

HU Jinqiu, DONG Shaohua, WANG Ronghan, ZHANG Xiyue

Department of Safety and Marine Engineering, China University of Petroleum-Beijing, Beijing 102249, China

引用格式：胡瑾秋, 董绍华, 王融涵, 张曦月 . 基于STAMP—STPA的LNG储备库典型事故正演模型构建 . 石油科学通报, 2021, 03: 481−493
HU Jinqiu, DONG Shaohua, WANG Ronghan, ZHANG Xiyue. STAMP-STPA based forward model construction of typical LNG repository accidents. Petroleum Science Bulletin, 2021, 03: 481-493. doi: 10.3969/j.issn.2096-1693.2021.03.039

Abstract In the absence of relevant accident probability statistics, in order to improve the overall safety of the Liquefied Natural Gas (LNG) system, we need to solve the problems that traditional safety analysis methods cannot consider. These are the internal correlation of complex systems, component interaction and macro control. The analysis ideas are scattered and we need to ensure the accuracy of the forward results of stratification, rollover and fire accident of LNG repositories, A STAMP-STPA (Systems-Theoretic Accident Model and Processes)- (Systems-Theoretic Process Analysis) based a forward model of typical LNG repository accidents was established, making the follow-up system of unexpected trouble analysis and accident cause analysis better and more comprehensive. First, according to the equipment and facilities, process and their correlation with each other involved in stratification and rollover accidents and fire accidents of LNG storage tanks, a preliminary risk analysis of the accidents was carried out, and then the factors leading to the accidents were identified, and the key nodes of the risk were ascertained. On this basis, the safety requirements and safety constraints of the accident system were analyzed, including control and feedback operations that may lead to accidents. A STAMP model was established which included the control and feedback relationships among the relevant facilities, components, and control feedback loops. Second, the STPA method was adopted to identify four unsafe control behaviors in the LNG safeguard process (including failure to provide control behavior, error or unsafe supply control behavior, failure to provide control behavior in a timely manner, and premature end of control behavior), and analyze the initial value (such as tank LTD parameter), current state (such as infusion operation) and state transition (such as tank and cooling completion preparation) involved in the overall process of the accident from two aspects of insufficient execution of control behavior, feedback error or insufficiency, and then understand the key causes of unsafe control behaviors, and established the complete forward model of typical accidents in LNG storage tanks. Finally, combined with specific accident cases to verify and analyze the effectiveness and practicality of the typical accident forward model of the LNG storage tank, and visualize the analysis results in the form of knowledge graphs. The study shows that the model can systematically analyze typical LNG accident processes of LNG tanks in complex systems from the perspective of control and constraints, which makes the accident evolution process more intuitive and the reasons for unsafe control behaviors clearer; and fully considers the causal relationship of various risk factors in the stratification, rollover and fire accidents forward from the system perspective, thus providing feasible and effective value information for the subsequent safety management of LNG storage tanks.

Keywords LNG repository; unsafe behavior; STAMP-STPA; fire accident; stratification and rollover accident

doi: 10.3969/j.issn.2096-1693.2021.03.039

0 引言

随着我国对天然气的需求的持续增长，为规避天然气供应不足或中断的风险，国家大力发展液化天然气储备库建设，并以大型液化天然气储罐储存各种类型的液化天然气产品。LNG具有易泄漏、易挥发扩散和易燃易爆等危险特性，LNG储备库存储了大量的液化天然气，是液化天然气储罐事故的集中发生地，它的安全问题早已成为业界最为关注的重要问题之一[1]。LNG的固有性质决定了其具有分层翻滚、火灾爆炸等危害特性。LNG分层翻滚事故是在LNG储存时由于分层而发生的一种剧烈蒸发过程，短时间内储罐压力由正常操作压力上升到压力安全阀设定压力，安全阀跳起向外排放天然气，大量BOG气体将以不可控制的速度迅速排至周围地区，若不能及时得以控制，将形成爆炸性混合云团，对LNG存储安全构成重大威胁[2]。自LNG进入工业应用以来，已经发生过多次翻滚事故，在 1970—1982 年之间，在 22 个工厂发生过 41 次翻滚事故，7 次作了正式报道[3]。LNG火灾事故也是LNG事故相关研究[4–7]关注的重点，因LNG挥发性强，能够迅速蔓延，遇到明火极易发生火灾；且容易引起多米诺事故的发生，造成爆炸、伤亡等更为严重的后果。基于以上内容，本文选择这 2 种事故作为LNG储备库典型事故进行系统性地安全性分析与事故正向演化研究，这对于LNG储备库的安全管理具有重要意义。

盛勇等[8]针对突发事件，从系统的复杂性、开放式预想及序贯性 3 个原则研究事件的情景演化机理，构建其演化系统模型；王海东等[9]用实际数据和情景构建方法进行建模，分析发生的可能性、发生发展方式和过程、可能产生的后果。针对传统的安全性分析方法存在的问题，N.G.Leveson等[10–11]提出了STAMP方法，并将其成功地应用在航空[12]、交通运输[13]等领域的安全问题上；国内王启全等[14]根据STAMP原理针对地铁突发事件引起人群恐慌而导致拥挤踩踏事故设计了应急联动系统，对地铁人群密度进行监控，以便在危险产生之前对人群进行应急疏散，从而减小了灾难发生的可能性。

通过上述研究发现，大多事故正演模型构建的研究仍较为传统，仅从事故发生条件和对事故机理进行微观描述，忽视组件交互及宏观控制；且STAMP模型在LNG典型事故正演方面的研究较少。鉴于此，笔者

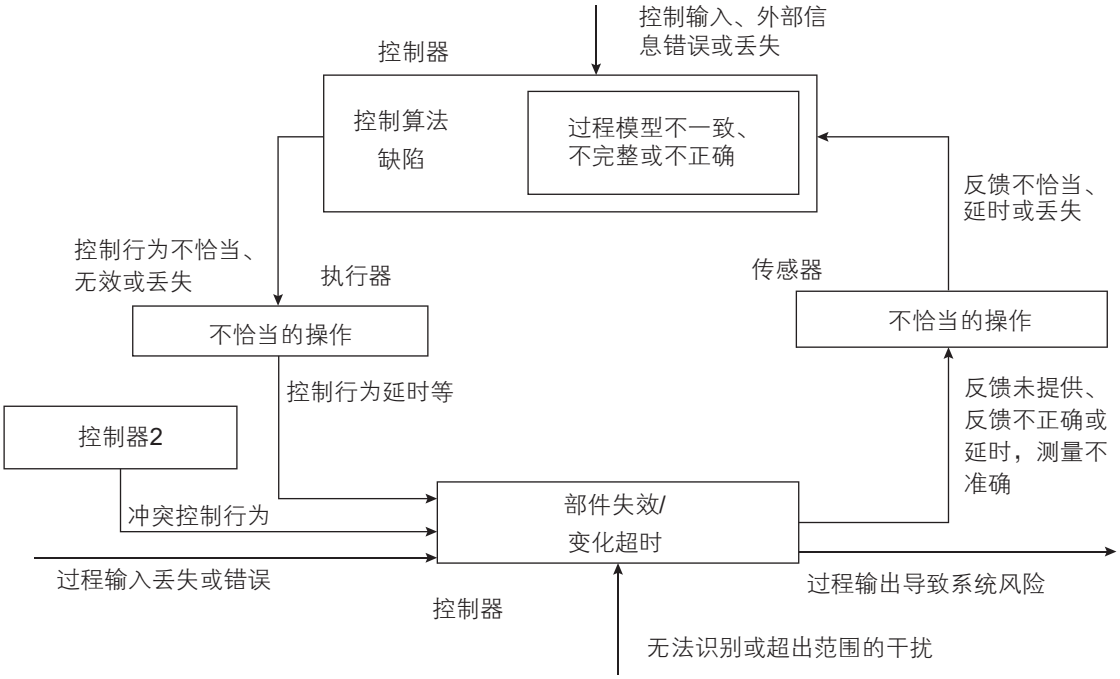

图 1　安全控制回路

Fig.1　Safety control loop

拟从系统控制的角度出发，结合STAMP—STPA模型对液化天然气事故过程进行安全性分析，以期系统性地构建LNG储备库分层翻滚及火灾事故正演模型。最后，在LNG储备库分层翻滚事故场景下，将建立的正演模型与常用的贝叶斯网络方法作对比，验证该模型在LNG储备库事故数据稀少的情况下，对于复杂系统在事故过程分析方面的优势。

1　STAMP—STPA 基本原理概述

1.1　STAMP 模型基本原理

STAMP模型于 2004 年由Leveson[10]提出，是基于系统理论和控制理论，将安全性视为系统组元、人为因素、环境因素和组织管理因素在非线性相互作用下的一种整体涌现性[15]。目前已在航空航天[16]、核电[17]和铁路[18]等行业的安全分析领域得到广泛应用。复杂系统作为一种开放的非线性系统，子系统之间以及系统与外界之间有物质、信息和能量的交互，安全评估的要点是要明确系统内部各种功能组件及其逻辑控制关系，分析组件可能遭遇的外部干扰和环境因素，从而明确系统正常运行所需的控制要求。

STAMP模型的 3 个基本概念是安全约束、分级安全控制结构和过程模型[19]。STAMP模型认为安全是一个控制问题[20]，并认为可能发生事故时，部件故障，外部干扰，以及异常交互作用的部件没有得到适当的控制。

1.2　STPA 基本原理

STPA是依赖于因果模型STAMP的系统性危害识别方法。STPA的目标是识别可能导致事故的不足的控制方案，从中可以将安全约束从系统概念推广到操作。STPA通过构建由控制器、执行器、控制过程和传感器构成的反馈控制回路[21]，如图 1 所示，分析控制行为在性能、时间或逻辑上的不合理情形，辨识不安全控制作用和场景。

STPA的执行包含以下步骤：1)辨识导致事故的系统状态或条件，定义系统风险；2)开发安全控制结构，识别系统元件之间的关联关系，分析安全需求和限制；3)识别不安全控制行为导致的约束失效(STPA定义了 4 种不安全控制行为：未提供控制行为、提供错误或不安全供控制行为、未及时提供控制行为、控制行为结束过早)；4)不安全控制行为关键原因分析。

与传统的安全分析方法对比(见表 1)，具体如表 1 所示，STAMP—STPA方法具有 3 个明显的优点：1)使安全研究人员能够考虑系统反馈的作用，以及根据反馈而采取的行动；2)结合了组织约束、技术约束和人员约束，并在同一级别内进行分析；3)能够通过框图理清事故在系统中的发展脉络，帮助安全管理者提高整个系统的安全性。

表 1 STAMP—STPA 与不同安全评价方法优缺点对比

Table 1 Comparison of advantages and disadvantages between STAMP—STPA and different security evaluation methods

	安全分析方法	性质	优点	缺点
1	FMEA	定性分析方法	简单，易上手	无法表示分析对象的内部联系
2	HAZOP	定性分析方法	通过引导词，启发管理者思维，激发想象力	对于复杂系统，难以成体系地进行安全分析
3	事故树	半定量分析方法	以图形演绎的方式，直观、便捷、有效地对故障状态作逐层深入分析	对于复杂系统，难以体现系统内不同部件间的联系
4	贝叶斯网络	定量分析方法	善于处理复杂系统中关联性和不确定性	无法表示系统内部的反馈过程；分析准确性依赖于历史统计数据
5	STAMP—STPA	定性分析方法	能够体现系统各组件间的反馈、控制过程；从系统的角度对系统整体进行分析	无法进行定量分析

2 LNG 储备库典型事故正演模型构建

与其他安全分析方法相似，STAMP—STPA 方法主要识别系统存在的风险，但不同之处在于该方法是能够考虑到不同设备间的交互，并通过分析系统的安全需求与安全性约束、辨识在事故演化过程中的不安全的控制行为，来识别系统控制回路中的不安全状态，从系统控制和约束的角度进行安全性分析。用 STAMP—STPA 方法进行事故正演模型构建，能够直观阐明事故发生过程，并保证事故正演模型的系统完整性。

2.1 LNG 储备库分层翻滚事故正演模型构建

基于 STAMP—STPA 的 LNG 储备库分层翻滚事故正演模型构建流程如下所示。

步骤 1：明确液化天然气储备库工艺流程

通过调查研究，明确研究对象主体、理清液化天然气储备库的工艺流程，并确定整体工艺流程中各部分设备设施的功能及相互间的关联关系。

步骤 2：分析 LNG 储备库分层翻滚事故的安全性

液化天然气分层翻滚事故发生在 LNG 储罐中，涉及到的设施包括储罐以及与储罐相关的管道、阀门、泵和 BOG 压缩机等。事故发生的主要原因有：罐内液体存储时间过长，罐壁或罐顶漏热，导致了不同位置的 LNG 温度不同，使温度大的液体向上流动，温度小的液体向下流动，罐内液体产生分层；在充注进料时，需充注的液化天然气和储罐内原有的液体密度和温度不同，不同密度的天然气在罐内产生分层。

步骤 3：分析安全需求和安全性约束

将罐内压力和 LTD 测点参数作为液化天然气分层翻滚的约束条件，通过相应的约束屏障对压力和 LTD 测点参数进行控制。如果液体在罐内分层后，能够及时通过温度、压力、密度测量仪器的反馈发觉，LNG 低压输送泵就可用于使罐内 LNG 液体循环，阻止液体分层向翻滚事故的演化；同时罐体周围设置的压力控制阀和安全放散阀可以在罐内压力过高或过低时，对罐内压力进行平衡，防止事故的进一步演化。

步骤 4：建立 LNG 储备库事故正演模型

对于液化天然气分层翻滚事故的控制和预防中，罐内液体的温度和罐内压力的控制是重点，因此对罐内液体的液位、温度、密度的监测尤为重要。采用 LTD 连续测量设施对罐内这 3 个参数进行监测，控制压力以防止罐内超压对储罐造成的结构损伤。根据图 1 的反馈控制回路，LNG 储备库作为复杂的人机系统，站内的操作人员和人工控制系统共同构成控制器，进液阀、BOG 压缩机、压力控制阀、安全阀和最小流量控制阀等组件的控制构成执行器，罐内压力和温度为控制过程，压力检测装置和 LTD 连续测量设施的反馈则为传感器。

结合 STAMP 模型，根据分层翻滚事故相关设备建立 LNG 储备库分层翻滚事故的正演模型，如图 2 所示。整个库区都在操作人员的监控指令下运行，下行箭头均为控制行为，上行箭头均为反馈过程。在接收到操作人员的充料指令后，执行器会依照指令执行，打开适合的进液阀门进液，LNG 储罐中的液位、温度、密度等信息会通过 LTD 仪表显示，并反馈给操作人员。如果产生分层，会对最小流量控制阀下达指令，使罐内泵执行循环操作，防止翻滚产生。当压力在正常范围内时，BOG 压缩机可从 BOG 通用管中提取气体，控制罐内的压力，并根据不同的大气压力调节罐的绝对压力。当罐内压力超过压缩机的调节范围之后，

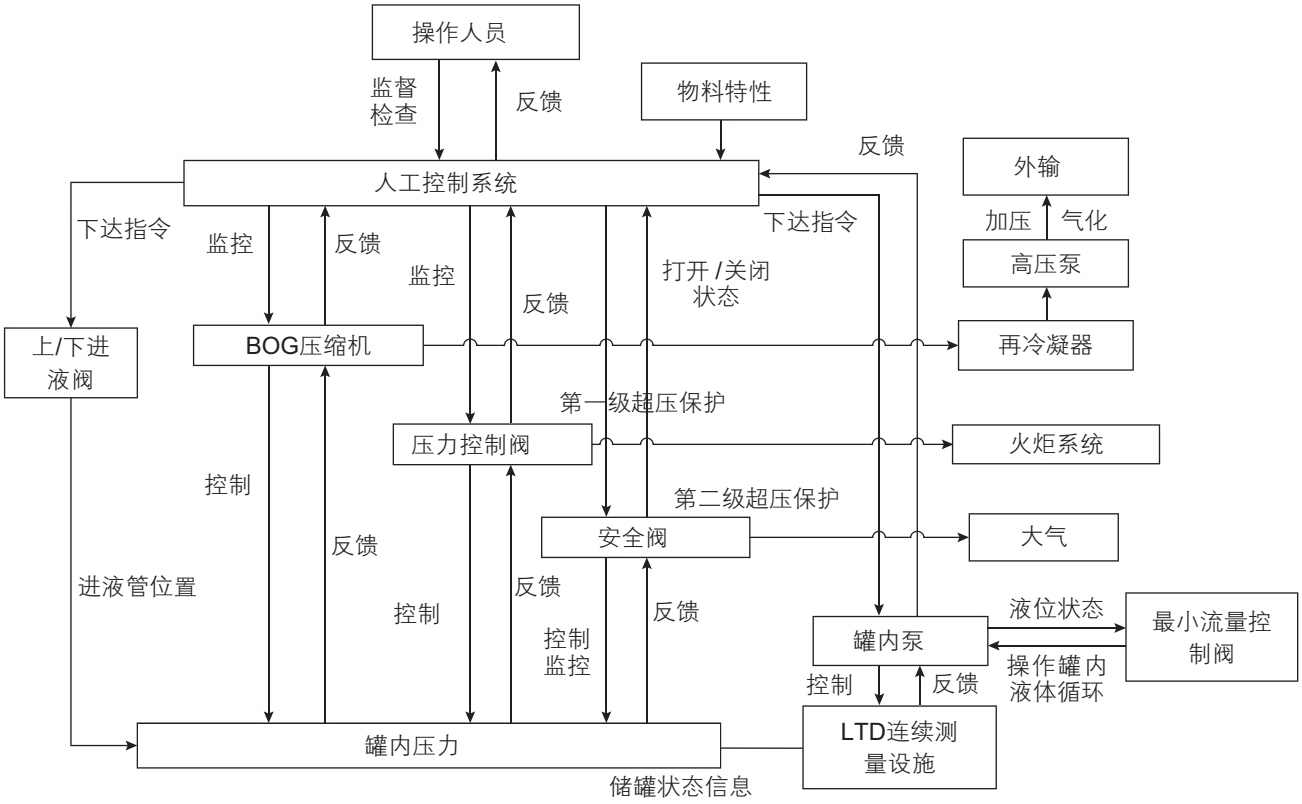

图 2 LNG储罐分层翻滚事故正演模型

Fig. 2 The stratification and rollover accident forward model of LNG tank

火炬系统发挥作用，气体通过压力控制阀阀门释放至火炬进行燃烧，这是第一级超压保护；当压力上升至更高水平时，安装在每个储罐中的多个泄压阀被打开，这是第二级超压保护。储罐状态信息继续传递，传回操作人员控制器，以此循环。

步骤 5：识别不安全控制行为

依据LNG储备库分层翻滚事故正演模型，从 4 类不安全控制行为角度，分析进料过程中储存系统中控制指令错误或不足导致的系统性风险，表 2 所示的不安全控制行为可转化为作用于罐内压力和液位的安全约束。为了防止分层翻滚事故的发生，在此过程中应保证系统控制行为符合安全约束。

步骤 6：关键原因分析

根据控制反馈模型以及STAMP—STPA提出的基本控制缺陷，总结不安全控制行为导致LNG储罐分层翻滚事故的关键原因：控制行为执行不充分、反馈信息错误或不足。其中，控制行为执行不充分包括：

(1)操作人员由于身体或心理原因执行控制指令不充分，导致操作失误。

(2)在罐内液体产生分层并下达循环操作指令后，罐内泵循环操作不彻底；定期检修制度不完善。

(3)罐内产生蒸发气体后，蒸发气的流量比压缩机的处理能力高时，压力控制阀未打开将超出部分蒸发气排到火炬，造成罐内超压，罐体破裂。

反馈信息错误或不足包括：

(1)反馈信息产生阶段：测量进料LNG密度、组分和罐内LNG密度的方式存在缺陷；系统各阀门状态信息的获取不充分或存在缺陷；其他与储罐进料时相关的重要信息没有及时获取或获取方法错误。

(2)反馈信息传输阶段：有关进料过程中罐内压力和罐内液体的液位温度密度差的反馈信息不正确；各级控制人员的反馈信息不正确、延时或丢失。

(3)外部因素影响：外部指挥信息不正确；站区环境温度、地形的获取不充分、不正确或丢失。

为验证此模型在复杂系统事故过程分析与事故正演模型建立方面的优势，将常用的事故概率模型贝叶斯网络用于该案例。该LNG储罐分层翻滚事故场景的贝叶斯网络如图 3 所示。

可以看出，在LNG储备库分层翻滚事故历史数据与资料稀少的情况下，事故中各节点的先验概率难以确认，此时定量的事故演化分析模型并不适用；且基于LNG储备库分层翻滚事故贝叶斯网络对该复杂系统进行事故过程分析，难以从系统的角度去看待问题，并且不能体现出系统各组件间的交互关联以及反馈信

表 2 不安全控制行为

Table 2 Unsafe control identification

不安全控制行为	导致的风险	安全约束
没有提供控制行为	进料前，没有确定新物料特性变化； 进料时，没有监测到超压和密度差过大等情况，导致分层翻滚； 液位不正常时，没有停止进料，导致超压或分层翻滚； BOG压缩机失效，导致超压； 到火炬的压力控制阀失效，完全打开，导致BOG排放到火炬； 安全阀失效，导致罐内超压； 最小流量控制阀和罐内泵失效，导致罐内液体无法充分混合导致分层翻滚事故； 压力检测变送器没有检测到压力异常；	定时检维修压力和LTD等监测装置，提高监测预警精度； 设置高低液位自动保护装置，当液位异常时，报警并联锁暂停充注物料； 定期检维修BOG压缩机和各个安全阀门和泵； 进料前，核对新物料温度密度参数；
控制行为错误或不安全	进液管位置选择错误，导致罐内液体混合不均匀，造成分层翻滚事故； 进料LNG组分不在合同规定的范围内，导致LNG大量闪蒸，发生分层翻滚； 温度检测变送器检测异常； 压力变送器误报警；	进料前确定进料的组分和罐内LNG密度； 利用低压输送泵混合密度不同的LNG；
控制行为发生延迟	到火炬的压力控制阀、安全阀失效，不能及时打开，导致罐内超压，进而损坏储罐； 最小流量控制阀没有及时打开循环，造成分层翻滚； 温度、压力、密度测量设施反馈不及时； 温度、压力、密度调节设施控制不及时； BOG没有及时泄压； 报警系统报警延迟；	定期查看各仪器仪表状态； 定期检修各仪器仪表； 设置压力报警阈值； 设置温度报警阈值； 设置密度差报警阈值； 定期检修报警系统； 建立完善的定期检修制度；
控制行为结束过早	LNG储罐上下进料阀关闭过早，导致无法正常进料； 安全阀泄压过早； 循环并关闭过早； BOG排放阀提前关闭；	进料前，确定进料阀阀位； 进料前确定罐内液体状态； 进料中时刻关注压力温度仪表反馈；

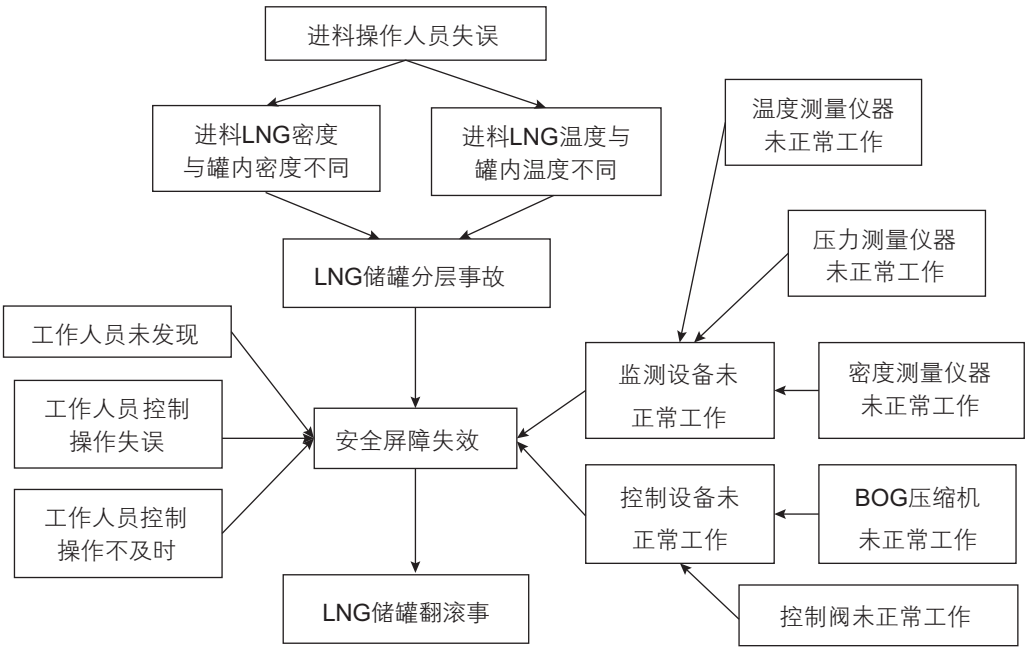

图 3 LNG储罐分层翻滚事故贝叶斯网络

Fig. 3 The stratification and rollover accident Bayesian network of LNG tank

息，使得系统事故信息不完善。

2.2 LNG储备库火灾事故正演模型构建

基于STAMP—STPA的LNG储备库火灾事故情景构建流程如下。

步骤 1：明确液化天然气储备库工艺流程

站内的操作人员和人工控制系统共同构成控制器，进液阀、BOG压缩机、压力控制阀、安全阀和最小流量控制阀构成执行器，罐内压力和罐区天然气气体浓度为控制过程，压力检测装置、罐体测温点和气体浓度监测系统则构成传感器。

步骤 2：分析LNG储备库火灾事故的安全性

罐区内的各种储存设施都是金属耐压罐，由于易受腐蚀或储罐存在先天性缺陷，加之安全管理措施不落实、维修保养不到位，极易造成储罐或零部件损伤，涉及到的设施包括管道、阀门、法兰盘接头、压缩机等，在发生意外时都有可能成为泄漏点，引起火灾爆炸事故；若储罐保温设施受到破坏，会造成低温保冷储存的LNG因受热而气化，储罐内的蒸汽压力剧增。正常情况下，安全放散阀自动开启，通过集中放散管释放压力，但若安全放散阀出现故障，储罐发生爆炸、火灾的可能性会大大增加。

步骤 3：分析安全需求和安全性约束

液化天然气火灾的约束条件是温度、压力和罐区气体浓度参数，通过相应的约束屏障对压力和温度进行控制。LNG储罐发生泄漏后，能够通过温度、气体浓度、压力测量仪器及时向总控制中心反馈异常温度、气体浓度变化、罐内压力波动等信息，防止事故向火灾演变。其中，通过气体浓度监测设备是最直接、快速地向人工控制系统反馈LNG储罐的泄漏的方式；罐体上的安全阀，压力检测阀门，可以及时调节罐内压力，预防罐内超压或破裂从而引起火灾爆炸事故。

步骤 4：建立LNG储备库事故正演模型

结合STAMP模型，得到LNG储备库火灾事故的正演模型，如图 4 所示。罐体测温点检测到温度异常时，反馈到人工控制系统；罐区内的气体监测系统随

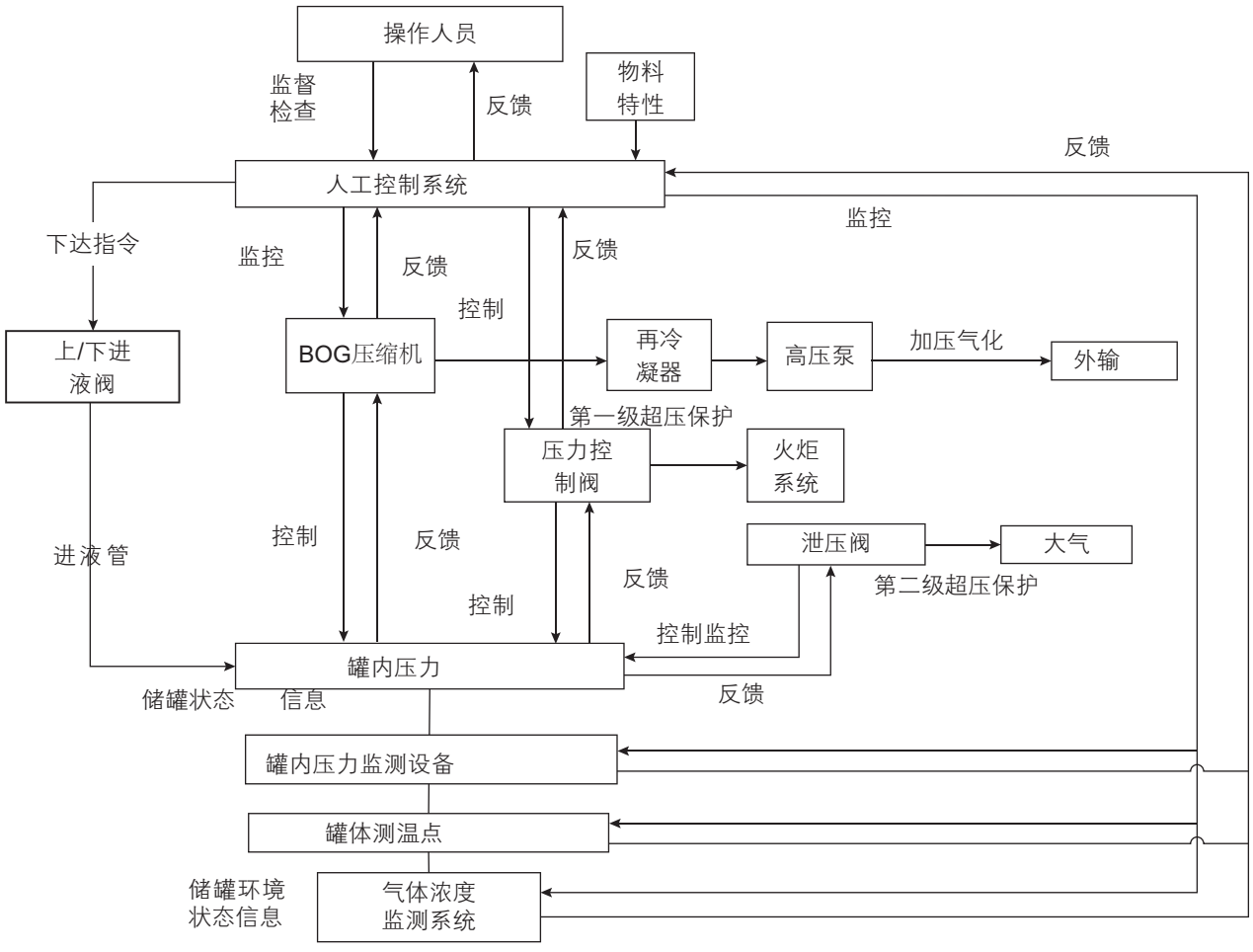

图 4 LNG储罐火灾事故正演模型

Fig. 4 The fire accident forward model of LNG tank

时监测罐区气体浓度状态，当气体浓度超过危险阈值时，报警反馈给人工控制系统。操作人员接收到反馈后，下达相应的指令找出气体浓度升高的原因，并及时做出响应。

步骤 5：识别不安全控制行为

依据LNG储备库火灾事故正演模型，从四类不安全控制行为角度，识别出的不安全控制行为如表 3 所示。为了防止事故的发生，在此过程中应保证系统控制行为符合安全约束。

步骤 6：关键原因分析

控制行为执行不充分包括：

(1)操作人员由于身体或心理原因执行控制指令不充分，导致操作失误。

(2)在罐内液体产生分层并下达循环操作指令后，罐内泵循环操作不彻底；定期检修制度不完善。

(3)罐内产生蒸发气体后，蒸发气的流量比压缩机的处理能力高时，压力控制阀未打开将超出部分蒸发气排到火炬，造成罐内超压，罐体破裂。

反馈信息错误或不足包括：

(1)反馈信息产生阶段：温度检测点反馈不及时；系统各阀门状态信息的获取不充分或存在缺陷；其他与储罐进料时相关的重要信息没有及时获取或获取方法错误。

(2)反馈信息传输阶段：有关进料过程中罐内压力和罐内液体的液位温度密度差的反馈信息不正确；各级控制人员的反馈信息不正确、延时或丢失。

表 3 识别不安全控制行为

Table 3 Unsafe control identification

不安全控制行为	导致的风险	安全约束
没有提供控制行为	进料前，没有确定新物料特性变化； BOG压缩机失效，导致超压； 到火炬的压力控制阀失效，完全打开，导致BOG排放到火炬； 安全阀失效，导致罐内超压； 压力检测变送器没有检测到压力异常； 温度检测变送器未检测到罐内LNG温度升高； 温度检测变送器监测到温度异常未报警； 火气系统逻辑设计错误，没有检测到泄漏的天然气； 火气系统失效，检测到泄漏没有报警； 低压泵失效，没有调节分层翻滚；	定时检维修压力和LTD等监测装置，提高监测预警精度； 设置高低液位自动保护装置，当液位异常时，报警并联锁暂停充注物料； 定期检维修BOG压缩机和各个安全阀门和泵； 进料前，核对新物料温度密度参数； 定期检测气体监测系统； 出入罐区佩戴气体检测器，穿戴专用的防护服和安全帽； 禁止携带易燃易爆物质进入罐区；
控制行为错误或不安全	进液管位置选择错误，导致罐内液体混合不均匀，造成分层翻滚事故； 进料LNG组分不在合同规定的范围内，导致LNG大量闪蒸，发生分层翻滚； 温度检测变送器检测异常； 压力变送器误报警； 火气系统误报警；	进料前确定进料的组分和罐内LNG密度； 利用低压输送泵混合密度不同的LNG；
控制行为发生延迟	到火炬的压力控制阀、安全阀失效，不能及时打开，导致罐内超压，进而损坏储罐； 最小流量控制阀没有及时打开循环，造成分层翻滚； 温度、压力、密度测量设施反馈不及时； 温度、压力、密度调节设施控制不及时； BOG没有及时泄压； 报警系统报警延迟； 气体浓度反馈延迟；	定期查看各仪器仪表状态； 定期检修各仪器仪表； 设置压力报警阈值； 设置温度报警阈值； 设置密度差报警阈值； 定期检修报警系统； 建立完善的定期检修制度；
控制行为结束过早	LNG储罐上下进料阀关闭过早，导致无法正常进料； 安全阀泄压过早； 循环并关闭过早； BOG排放阀提前关闭；	进料前，确定进料阀阀位； 进料前确定罐内液体状态； 进料中时刻关注压力温度仪表反馈；

(3)外部因素影响：外部指挥信息不正确；站区环境温度、地形的获取不充分、不正确或丢失，设计缺陷；自然灾害。

3 案例分析

本部分先通过国外BG公司Partington LNG调峰站发生分层翻滚事故验证LNG储备库典型事故正演模型的可行性、有效性与准确性；再通过仿真的国内LNG接收站储罐火灾事故验证此模型的普适性。

3.1 LNG储罐分层翻滚事故案例分析

案例场景描述：1993 年 10 月，BG公司Partington LNG调峰站发生分层翻滚事故，该调峰站包含 2 套天然气液化设施，4 座 5×10^4 m^3 的LNG储罐。在一次卸料充注的过程中充注的LNG密度为 433 kg/m^3，比储罐原有的液体密度高 13 kg/m^3，LNG加液量为 1900 t。进料完成后，经过 68 d储存，罐内液体突然翻滚，导致储罐上的安全释放阀和紧急排放阀全部打开。整个事故过程中，气体翻滚排放持续了 2 h，储罐设置排放天然气的总能力是 123.4 t/h，高于此次事故排放平均质量流量 75 t/h，所以没有造成储罐罐体损伤。此次排放量是正常排放量 0.25 t/h的 300 倍，造成了大量的物料损耗。

结合图 2 所示模型，建立本事故场景的LNG储罐分层翻滚事故正演模型，如图 5 所示，结合该模型对此案例进行分析，可以发现此系统中存在的问题及原因有：

(1)操作人员未掌握物料信息

操作人员进行充注操作前未掌握需要充注的LNG的物料信息和罐内已有LNG液体的物料信息。可能的原因是：①企业操作规程不完善；②操作人员由于自身原因出现疏漏；③企业安全文化教育不全面。

(2)操作人员未意识到存在此密度差时进行充注操作存在的安全隐患

操作人员在此情况下对控制系统下达了进料指令，且选择了打开上进液阀进液。可能的原因有：①企业安全文化教育不全面；②操作人员自身知识学习不到位；③企业操作规程不完善。

(3)操作人员未及时发现分层现象

操作人员未从储罐状态信息反馈设施中发现分层现象的发生。发生此情况的原因为：①操作人员由于自身原因出现疏漏；②储罐状态信息反馈不明显；③企业安全文化教育不全面。

将正演模型分析结果与事故调查得到的原因进行对比，具体如表 4 所示，可以发现：通过LNG储备库

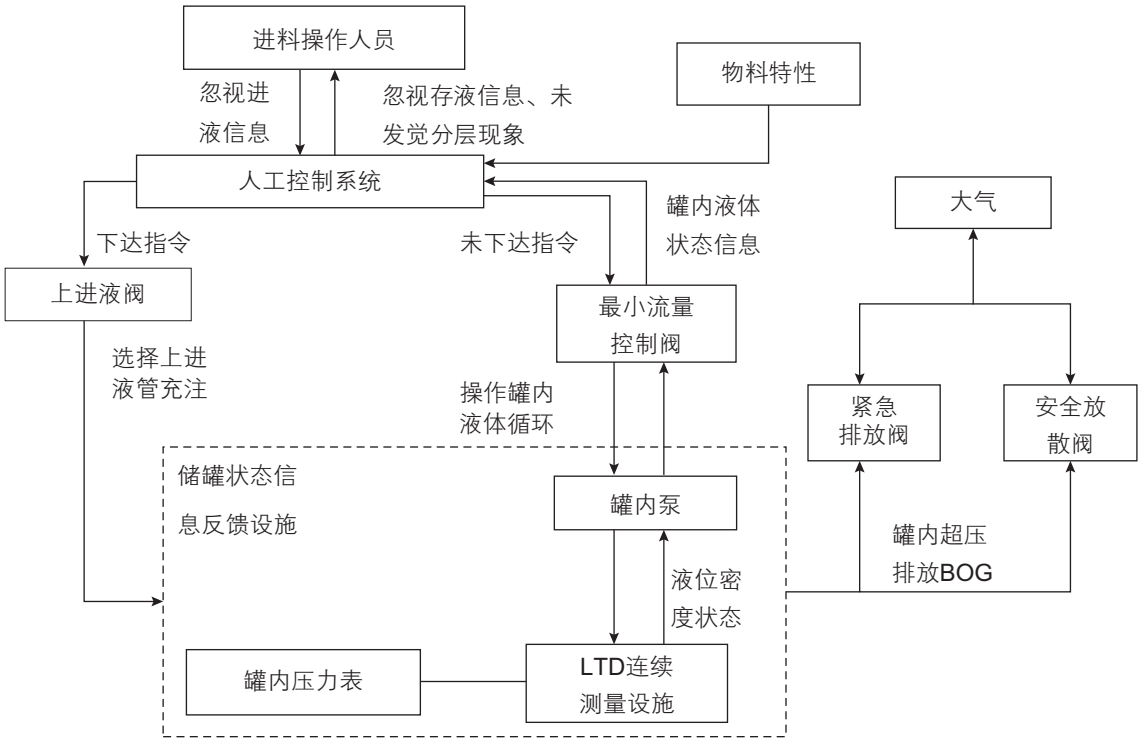

图 5 本案例场景的事故正演模型

Fig. 5 The accident forward model of the case scenario

典型事故正演模型分析得到的结果更加注重整个事故中涉及到的关键要素间的联系与相互作用造成的事故后果，例如，“操作人员没有对分层反馈及时采取有效操作”这一原因中涉及“操作人员”、“储罐状态设施反馈(分层反馈)”和“循环操作(有效操作)”3 个关键要素，而不仅仅是单一原因。因此，通过正演模型分析得到的事故原因不仅更加具体、全面、有针对性，且能够保证分析结果的准确性。

最后，为直观的体现此模型在火灾事故案例安全性分析方面的全面性与系统性，以知识图谱的方式，将案例中各原因之间的逻辑层次与内部因果关联进行可视化，如图 6 所示。其中，橙色的节点对应上文中所写的此系统中存在 3 个方面的问题；蓝色的节点代表导致问题发生的原因；连线表示各节点间的关联关系。

3.2 LNG 储罐火灾事故案例分析

案例场景描述：某LNG接收站LNG储罐底由于设计缺陷和检修不合格等外部因素发生泄漏后，气体检测装置没有产生报警信息，泄漏气体在局部达到一定浓度后遇火源，发生火灾。结合图 4 所示模型，建立本事故场景的LNG储罐火灾事故正演模型，如图 7 所示。

不同于人员操作失误等原因造成罐内压力不稳定而间接导致的泄漏，此事故案例是由于设计缺陷和日常检修不合格等外部因素导致罐底发生泄漏，因此，此场景下系统无法通过罐内压力监测设备对泄漏的发生进行预警。结合建立的火灾事故正演模型对案例进

表 4 案例事故调查和模型分析得到的事故原因对比

Table 4 The comparison of accident causes from accident investigation and model analysis

事故原因	案例事故调查结果	正演模型分析结果
相同	采用了上进液方式，阻止了下层LNG液体的蒸发；罐内原有液体和新LNG密度相差 13 kg/m^3，使罐内出现分层；	采用了上进液方式使下层LNG蒸发受阻，导致分层；操作人员掌握物料信息不足，注入与罐内原有液体存在密度差的新物料；
差异	调峰站储存LNG时间过长。	操作人员忽略储罐状态信息设施分层反馈；操作人员没有及时对分层反馈采取有效操作。

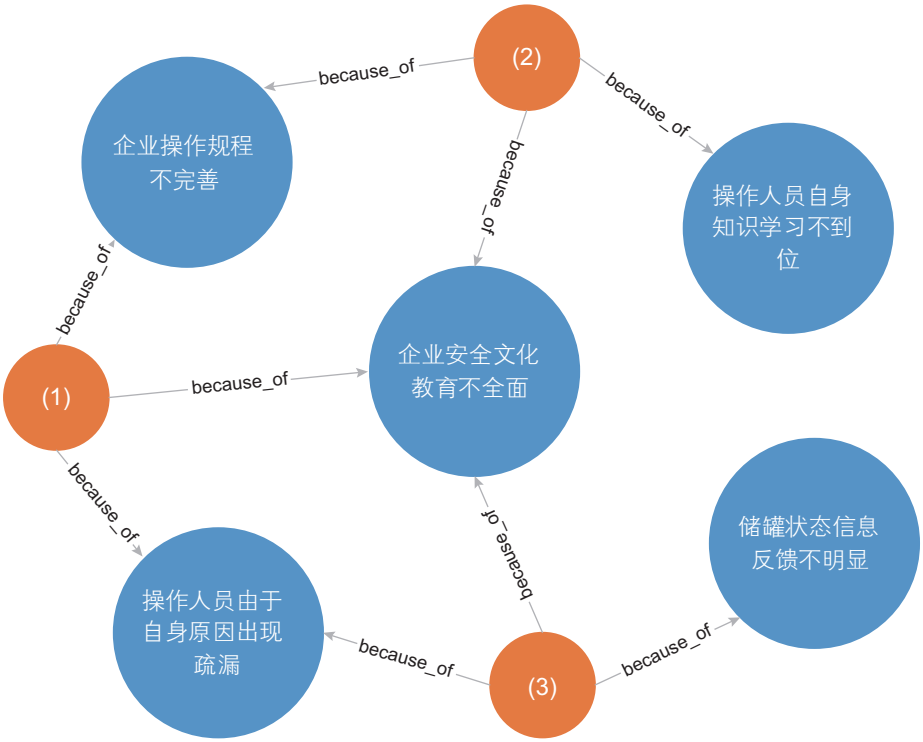

图 6 LNG 分层翻滚事故案例原因的关联知识图谱

Fig. 6 Correlation knowledge graph of LNG stratification and rollover accident causes

行分析，可以发现此系统中存在的问题及原因有：

(1)气体浓度监测系统未产生报警信息

该安全问题有两方面的原因：①检测装置自身失效，丧失基本功能；②检测装置的设计存在缺陷，即泄漏点属于气体浓度检测系统的盲点。

(2)罐底的测温点的传感器出现异常

该安全问题有两方面的原因：①传感器自身失效，无法检测到泄漏点的温度；②检测装置的设计存在缺陷，即无法检测到泄漏点的异常温度。

(3)罐内压力监测设备反馈不及时

若在泄漏初期能及时反馈罐内压力波动情况，可以在发生火灾事故前对泄漏进行控制。发生此安全问题的原因可能有：①储罐泄漏前期压力波动不明显，罐内压力监测设备无法及时进行反馈；②压力监测设备本身灵敏度不足，无法检测泄漏量较少的压力波动；③总控制系统存在缺陷，未能准确区分泄漏与正常压力波动，无法产生报警信息。

对以上 3 点系统设备原因进行进一步分析，可以得到以下安全管理方面的问题及原因：

(4)维检修人员出现工作漏洞

出现此类安全问题的原因可能是：①人员日常维检修制度不完善；②工作人员本身当天的生理或者心理状态不佳；③罐区安全管理制度规程不完善。

(5)罐区存在外部火源

由于外部点火源LNG泄漏事故产生后，导致演变成火灾事故，出现此类安全问题的原因有：①罐区对火源的控制存在漏洞；②罐区防静电措施不足；③人员安全教育不到位。

可以看出，本文提出的基于STAMP—STPA的LNG储备库典型事故正演模型适用于LNG储备库的所有事故类型，具备普适性，可以广泛使用。

将案例中各原因之间的逻辑层次与内部因果关联进行以知识图谱的形式可视化，结果如图 8 所示。从图中可以看出，在此系统中，“气体浓度监测系统未产生报警信息”、“罐底的测温点的传感器出现异常”、“维检修人员出现工作漏洞”和“罐区存在外部火源”有明显的内部因果关联；最终的LNG储罐火灾事故原因聚焦在罐区的安全管理及制度规范方面，为LNG储备库后续的安全管理工作提供了清晰的整治方向。

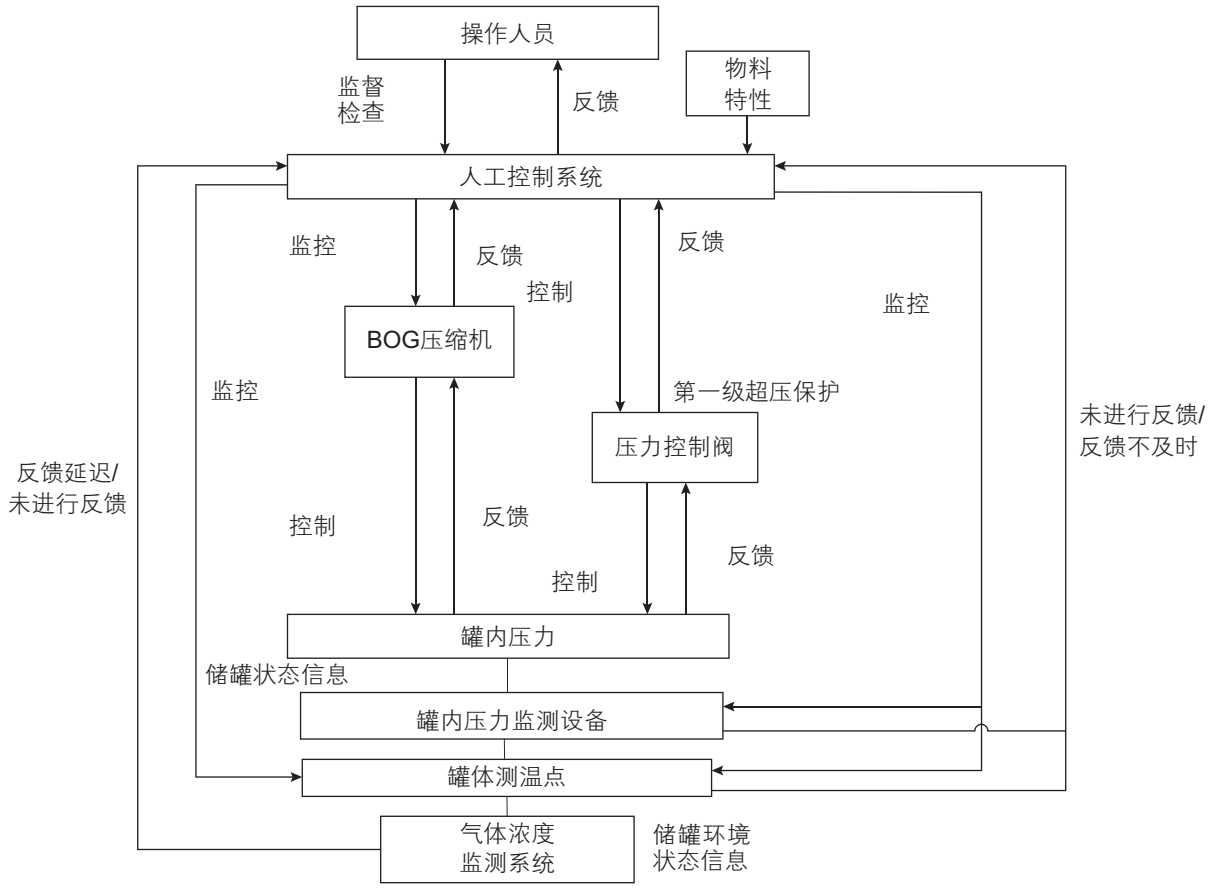

图 7　本案例场景的事故正演模型

Fig. 7　The accident forward model of the case scenario

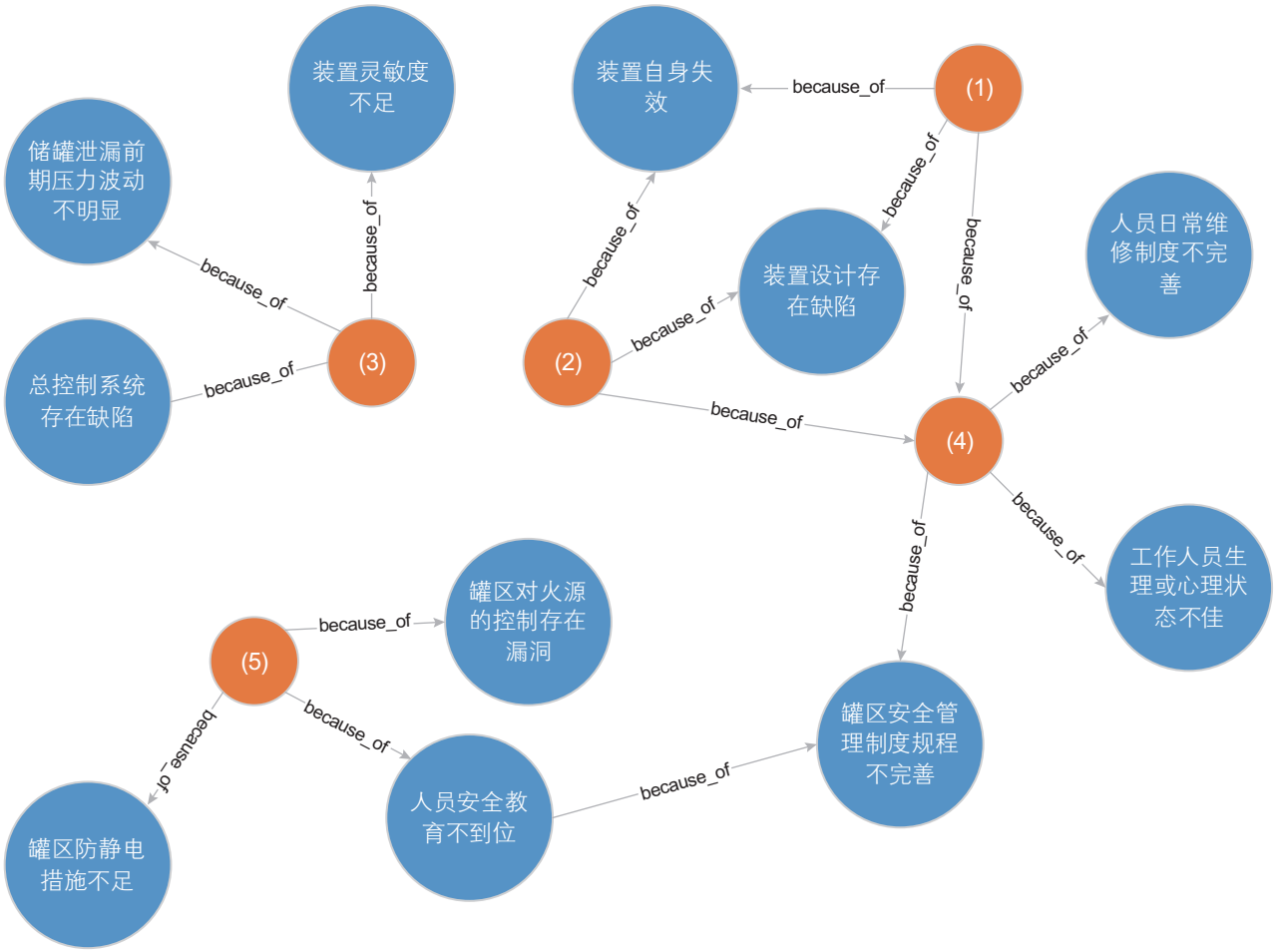

图 8 LNG 火灾事故案例原因的关联知识图谱

Fig. 8 Correlation knowledge graph of LNG fire accident causes

4 结论

(1) 本文提出的基于STAMP—STPA的LNG储备库典型事故正演模型，针对LNG储备库具体工艺流程特点，通过安全控制结构的定义以及系统风险和约束的辨识，实现了不安全控制行为的有效识别及其关键原因的深度挖掘。

(2) 基于STAMP—STPA的LNG储备库典型事故正演模型克服了传统安全性分析方法无法考虑复杂系统内部关联性、忽视组件交互及宏观控制等问题，使得系统隐患分析、事故原因溯源更加全面完善。

(3) 基于STAMP—STPA模型，从系统控制的角度出发分析LNG储备库分层翻滚、火灾事故安全性及演化过程，使得分层翻滚与火灾事故场景更加直观、原因及内部因果层次关系梳理更加清晰，同时也为后续的事故反演研究打下基础。

参考文献

[1] 曹广明. LNG接收站事故统计分析研究[J]. 安全、健康和环境, 2014, 14(07): 9−11. [CAO G M. Statistical analysis of LNG receiving station accidents [J]. Safety Health & Environment, 2014, 14(07): 9−11.]

[2] 金春旭, 潘振, 陈保东, 等. 液化天然气储罐翻滚事故分析[J]. 当代化工, 2014, 43(10): 2065−2067. [JIN C X, PAN Z CHEN B D, et al. Analysis of LNG storage tank rollover accidents[J]. Contemporary Chemical Industry, 2014, 43(10): 2065−2067.]

[3] SHI J Q. Numerical modeling and experimental study of rollover in cryogenic liquids and liquid freon, UK: University of Southampton, 1991.

[4] 于庭安, 戴兴国. LNG储罐火灾和爆炸事故树分析[J]. 中国安全科学学报, 2007(08): 110−114+177. [YU T A, DAI X G. Fault tree

analysis of fire & blast accidents caused by LNG tanks[J]. China Safety Science Journal, 2007(08): 110−114+177.]

[5] 杨新顺. LNG储备库风险评价研究[J]. 山东工业技术, 2014(15): 152. [YANG X S. Research on risk assessment of LNG reserves[J]. Shandong Industrial Technology, 2014(15): 152.]

[6] 刘应春, 霍家莉, 张彬. 液化天然气泄漏扩散和池火灾害研究现状与展望[J]. 南京工业大学学报(自然科学版), 2019, 41(05): 664−671. [LIU Y C, CUI J L, ZHANG B. Perspective on liquefied natural gas leakage diffusion and pool fire research development[J]. Journal of Nanjing Tech University(Natural Science Edition), 2019, 41(05): 664−671]

[7] 党文义. 大型LNG储罐全面积火灾研究[J]. 消防科学与技术, 2017, 36(05): 606−609. [DANG W Y. Research on the full-surface pool fire of large LNG storage tank[J]. Fire Science and Technology, 2017, 36(05): 606−609.]

[8] 盛勇, 孙庆云, 王永明. 突发事件情景演化及关键要素提取方法[J]. 中国安全生产科学技术, 2015, 11(1): 17−21. [SHENG Y, SUN Q Y, WANG Y M. Emergency scenario evolution and extraction method of key elements[J]. Journal of Safety Science & Technology, 2015, 11(1): 17−21.]

[9] 王海东, 陈凯, 安广海, 等. LNG船舶港口泄漏事故情景构建及危害程度分析[J]. 中国安全生产科学技术, 2019, 15(05): 173−178. [WANG H D, CHEN K, AN G H, et al. Analysis on hazard degree of leakage accident of LNG ship in port based on scenario construction[J]. Journal of Safety Science & Technology, 2019, 15(05): 173−178.]

[10] LEVESON N G. A Systems-Theoretic approach to safety in software-itensive systems[J]. IEEE Transactions on Dependable & Secure Computing, 2004, 1(1): 66−86.

[11] LEVESON N. A new accident model for engineering safer systems[J]. Safety Science, 2004, 42(4): 237−270.

[12] FLEMING C H, Leveson N G. Early concept development and safety analysis of future transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, PP(99): 1−12.

[13] SALMON P M, READ G J, STEVENS N J. Who is in control of road safety? A STAMP control structure analysis of the road transport system in Queensland, Australia[J]. Accident Analysis & Prevention, 2016, 96: 140−151.

[14] 王起全, 王鸿鹏. 基于情景构建的危化品事故应急疏散模拟研究[J]. 中国安全科学学报, 2017, 27(12): 147−152. [WANG Q Q, WANG H P. A scenario construction based study on emergency evacuation in hazardous chemicals accident[J]. China Safety Science Journal, 2017, 27(12): 147−152.]

[15] 孟祥坤, 陈国明, 张肖锦, 等. 深水井控STAMP/STPA安全性分析[J]. 中国石油大学学报(自然科学版), 2019, 43(02): 131−139. [MENG X K, CHEN G M, ZHANG X J, et al. Safety analysis of deepwater well control based on STAMP /STPA[J]. Journal of China University of Petroleum, 2019, 43(02): 131−139.]

[16] 王瑛, 孙赟, 李超, 朱法顺, 等. 基于STAMP模型的军机飞行训练安全性分析[J]. 中国安全科学学报, 2018, 28(09): 68−73. [WANG Y, SUN Y, LI C, ZHU F S, et al. Analysis of military aircraft flight training safety based on STAMP model[J]. China Safety Science Journal, 2018, 28(09): 68−73.]

[17] 刘杰, 阳小华, 余童兰, 等. 基于STAMP模型的核动力蒸汽发生器水位控制系统安全性分析[J]. 中国安全生产科学技术, 2014, 10(5): 78−83. [LIU J, YANG X H, YU T L, et al. Safety analysis on control system for water level of steam generator in nuclear power plant based on STAMP model［J]. Journal of Safety Science and Technology, 2014, 10(5): 78−83.]

[18] DONG A. Application of CAST and STPA to railroad safety in China[D]. Cambridge: Massachusetts Institude of Technology, 2012.

[19] GONG Y H, LI Y T. STAMP-based causal analysis of China-Donghuang oil transportation pipeline leakage and explosion accident[J]. Journal of Loss Prevention in the Process Industries, 2018.

[20] 祝楷. 基于系统论的STAMP模型在煤矿事故分析中的应用[J]. 系统工程理论与实践, 2018, 38(04): 1069− 1081. [ZHU K. Application of STAMP model in coal mine accident analysis[J]. Systems Engineering-Theory & Practice, 2018, 38(04): 1069−1081.]

[21] 郑磊, 胡剑波. 基于STAMP/STPA的机轮刹车系统安全性分析[J]. 航空学报, 2017, 38(1): 241−251. [ZHENG L, HU J B. Safety analysis of wheel system based on STAMP/STPA[J]. Acta Aeronautica Sinica, 2017, 38(1): 241−251.]

(责任编辑　王雨墨　编辑　马桂霞)