石油科学通报
Petroleum Science Bulletin

安全思维和事故模型研究分析与展望

伍星光，侯磊*，刘芳媛，吴守志，伍壮

中国石油大学(北京)油气管道输送安全国家工程实验室/石油工程教育部重点实验室，北京 102249
* 通信作者, houleicup@126.com

收稿日期: 2019−11−16
国家重点研发计划(2016YFC0802104, 2017YFC0805800) 资助

摘要　社会技术系统的日益复杂不仅滋生了更多潜在的安全问题，也促进了安全思维的不断改变。安全思维由基于事后响应的被动式管理向基于实时监控的主动式管理转变，事故模型也从简单线性思维发展到复杂系统思维。对事故模型功能和内涵的深刻理解有助于针对具体实际问题进行模型优选与开发。目前鲜有研究对安全思维及其与事故模型的关系进行深入探究，缺乏对各事故模型的特点、适用性和局限性的综合分析。本文在总结分析安全理念和思维发展历程的基础上，将事故模型划分为基于事件的因果链式模型、基于系统理论的事故模型和基于安全屏障的事故预测模型，从模型起源、功能和适用性等方面对 3 类模型中的代表性模型进行了综合分析，通过对比不同类别模型的优缺点和应用前景，展望了事故模型面临的挑战和未来的发展方向。

关键词　社会技术系统；安全思维；事故模型；链式模型；系统理论；安全屏障

The analysis and prospects of safety thinking and accident models

WU Xingguang, HOU Lei, LIU Fangyuan, WU Shouzhi, WU Zhuang

National Engineering Laboratory for Pipeline Safety/MOE Key Laboratory of Petroleum Engineering,China University of Petroleum-Beijing, Beijing 102249, China

Abstract　The increasing complexity of social-technical systems has not only created more potential safety issues, but has also spurred constant changes in safety thinking. Safety thinking has changed from reactive management based on post-event response to proactive management based on real-time monitoring, while the accident models have also changed from simple linear thinking to complex system thinking. Profound understandingof the function and connotation of the accident model is helpful for model selection and development for specific practical problems. To date, little work has been done to conduct in-depth analysis of safety thinking and its relationship with accident models, and the characteristics, applicability and limitations of each accident model. In this study, on the basis of the review of the development of safety concepts and safety thinking, the accident models were divided into event-based causal chain models, models based on system theory and predictive models based on safety barriers. Representative models of the three types were comprehensively analyzed from the aspects of model origin, function, and applicability. The challenges and future development directions of the accident models were reviewed by comparative analysis of the advantages, disadvantages and application prospects of different types of models.

Keywords　social-technical system; safety thinking; accident model; chain model; system theory; safety barrier

doi: 10.3969/j.issn.2096-1693.2020.02.022

引用格式：伍星光, 侯磊, 刘芳媛, 吴守志, 伍壮. 安全思维和事故模型研究分析与展望. 石油科学通报, 2020, 02: 254−268
WU Xingguang, HOU Lei, LIU Fangyuan, WU Shouzhi, WU Zhuang. The analysis and prospects of safety thinking and accident models. Petroleum Science Bulletin, 2020, 02: 254-268. 10.3969/j.issn.2096-1693.2020.02.022

0 引言

安全是人们免于受伤害的现实需求和心理需求。为了掌控系统安全性变化趋势以及预防不期望事件发生，人们通常基于大量真实事故分析及行业经验，建立能够表征原因和后果关系的事故模型。事故模型提供了理解事故的发生发展方式的参考框架，能为系统开发过程风险评估以及事后事故分析提供技术性指导。

事故模型从最早的多米诺骨牌模型发展至今已有数十种之多，每种模型都有各自的特点和适用范围。覃容和彭冬芝[1]将事故致因理论分为单因素事故理论、事故因果连锁论、流行病学理论和系统理论四种，分别讨论了各理论的主要观点以及相应事故模型的特点。罗春红和谢贤平[2]对比分析了2000年前的一些事故致因理论和事故模型，并运用不同的事故致因理论定性分析具体事故案例。陈宝智和吴敏[3]阐述了从事故频发倾向论到系统理论事故模型不同时间段的安全背景和安全理念。这些研究更多是对事故致因理论的回顾，并未深入讨论事故模型的功能特点和研究现状。傅贵等人[4]对比分析了10种主流的事故模型，从事故影响对象、模型架构和事故发生路径3个维度阐述了各模型的优劣以及适用范围。该研究关注事故模型的组成结构和选用依据，并未结合时代背景深入探讨事故模型的理论内涵和安全思维。不同的事故模型是基于不同的安全需求产生的，每个事故模型又都蕴含着思考安全的方式，只有综合理解模型功能和安全思维才能帮助分析者做出正确有效的选择，推动事故模型向更完善的方向发展。Qureshi[5]对2007年以前的主流事故模型进行了详细的分类和描述，并展望了事故模型面临的挑战和发展趋势。然而，该研究由于是2007年发表，并未涉及最新的事故预测模型。本文对安全理念和思维的发展历程进行全面回顾，基于不同的安全思维对事故模型进行分类，通过综合分析不同事故模型的特点和局限性，展望事故模型的发展趋势。由于本文更关注社会技术系统的整体模型，所涉及的模型范围没有涵盖人的因素模型。

1 安全理念和思维的发展历程

在科技落后的时代，人们往往认为天灾人祸是“命中注定”且无法控制的。直到第二次工业革命之后，风险和安全的概念和影响才真正意义上受到世人关注。安全科学发展至今，大致经历了5个阶段[6–8]，分别是技术时代、人的因素时代、管理体系时代、整合性时代和适应性时代。

(1)技术时代(19世纪30年代到20世纪50年代)：在工业革命之后，技术的不可靠性为人类生活引入了新的风险，事故主要归因于机械故障和结构失效，事故预防的重点是通过消除、替代或隔离潜在危害从源头控制风险。在此阶段，人们对于事故过程的理解和事故原因的分析主要基于海因里希的多米诺骨牌理论，概率风险评估(Probabilistic Risk Assessment)逐渐兴起并成为系统安全性评估和可靠性分析的主要方法。

(2)人的因素时代(20世纪50年代到20世纪80年代)：在技术时代，人的行为由于过于不精确而难以预测的特性被视为技术生产的限制性因素。因此，人们致力于发展自动化技术以弱化人的角色。在第二次世界大战之后，尤其是在1979年美国三哩岛核电站事故发生后，组织管理者开始意识到通过技术发展并不能排除所有风险，将注意力逐渐转向人机交互的设计和研究。

(3)管理体系时代(20世纪80年代到2000年)：1986年发生的“挑战者号”航天飞机事故和切尔诺贝利核电站事故后，线性因果范式和简单的人机交互理念受到了质疑。一系列沉痛的教训清楚地表明，人的表现源于社会技术系统中各因素复杂的相互作用，很多时候并不是事故或错误的唯一原因。在风险评价和安全管理中，开始将具体的组织因素纳入分析范围。

(4)整合性时代(2000年至今)：随着科学技术的不断发展，工业系统中的要素变得越来越复杂精细和紧密耦合，人们逐渐意识到不良的组织文化因素在许多事故中起着至关重要的作用。在此阶段，研究者们指出更完善合理的事故模型的建立不应轻易摈弃每个发展时期的思维模式，也不应偏重技术因素、人的因素和组织因素中的任一因素，需要基于兼容并包的思想对各个时期的安全分析理念和方法进行整合。

(5)适应性时代(2010年至今)：适应性时代强调安全和事故是互补关系，不仅要关注系统为什么出错，也要关注怎样使系统成功运转。有效的安全管理策略不仅要能在事后提供改进的意见，更要在事前对系统可能的安全状态做出预测。这就要求高级管理者不要依赖于自身所想象的来完成工作，而是要经常与一线工人进行坦诚沟通，了解他们的工作现状和系统的变化情况。

这5个时代所包含的关于事故原因的探索和安全机制的思考本质上体现了两种思维模式的变化，即丹麦Hollnagel教授所提出的安全I和安全II的概念[9]。安

全I对应的安全性定义是不良后果数量尽可能少的条件水平。从安全I的角度来看，安全管理的目的是确保事故或异常事件数量在合理可行的范围内尽可能少。这意味着安全管理必须从缺乏安全性开始，通过事后分析确定系统出错的地方并加以控制和改进。安全I所基于的最重要的假设是所有不良结果都有对应的原因，且总能通过推理找到结果对应的前一阶段的原因。这种事故因果关系的信条由于简单易行以及便于法律上的追责而被人们广泛遵循[10−11]。由于事故分析目的是从最终结果倒推以找到失效的组件，基于事件的因果链式模型在这种环境下应运而生，其中以多米诺骨牌模型(Domino Model)[12]和瑞士奶酪模型(Swiss Cheese Model)[13]最为著名。在漫长的时间里，这种以事故结果为驱动辨识系统脆弱性的被动式安全管理理念根深蒂固。然而，不断增加的交互复杂性和耦合性使设计人员和操作人员难以考虑所有潜在的系统状态[14]，且在某一个系统中完全安全的组件在另一个系统中可能并不安全[15]。如果发生了无法预知和无法想象的“黑天鹅事件”，即使拥有一套现成的紧急响应措施也将无济于事[16−17]。因此，需要启发式方法和更综合性的模型来应对不断变化的实际情况[15,18]。这种主动式管理的需求推动了安全II的产生。

安全II是对安全I的补充，将安全的定义从“避免出现问题”更改为“确保一切都正确”，即弹性恢复力工程(Resilience Engineering)中定义的不同条件下取得成功的能力[19−20]。从安全II的角度看，安全管理的目的是确保事情日常工作尽可能正确，而不仅仅是关注错误的事情。两种安全思维的区别在于安全I将事故视为结果性(Resultant)的现象，是一系列事件相继发生的结果；安全II认为事故是突发性(Emergence)的现象，是系统各组件负效应综合作用的瞬时结果，不能将其追溯到特定原因或功能[9,15,19,21]。因此，主动性的安全管理需要更多发挥人的主观能动性，通过不断学习克服设计缺陷和功能故障，监控每日自身和系统的变异性并及时做出调整。基于系统理论的事故模型就是安全II时代的产物，其中具有代表性的模型有社会技术系统风险管理框架(Socio−Technical Risk Management Framework)[22]、基于系统理论的事故模型与过程(STAMP, Systems-Theoretic Accident Model and Processes)[23]和功能共振分析方法(FRAM，Functional Resonance Analysis Method)[24]。针对现有系统事故模型缺乏定量过程的局限性，相关学者又开发了基于安全屏障的事故预测模型，主要有过程事故模型(Process Accident Model)[25]、系统危害识别、预测和预防模型(SHIPP, System Hazard Identification, Prediction and Prevention)[26]和基于安全屏障的非序列模型(Non−Sequential Barrier−Based Process Accident Model)[27]。图 1 展示了安全思维和安全模型的发展进程和相互关系。

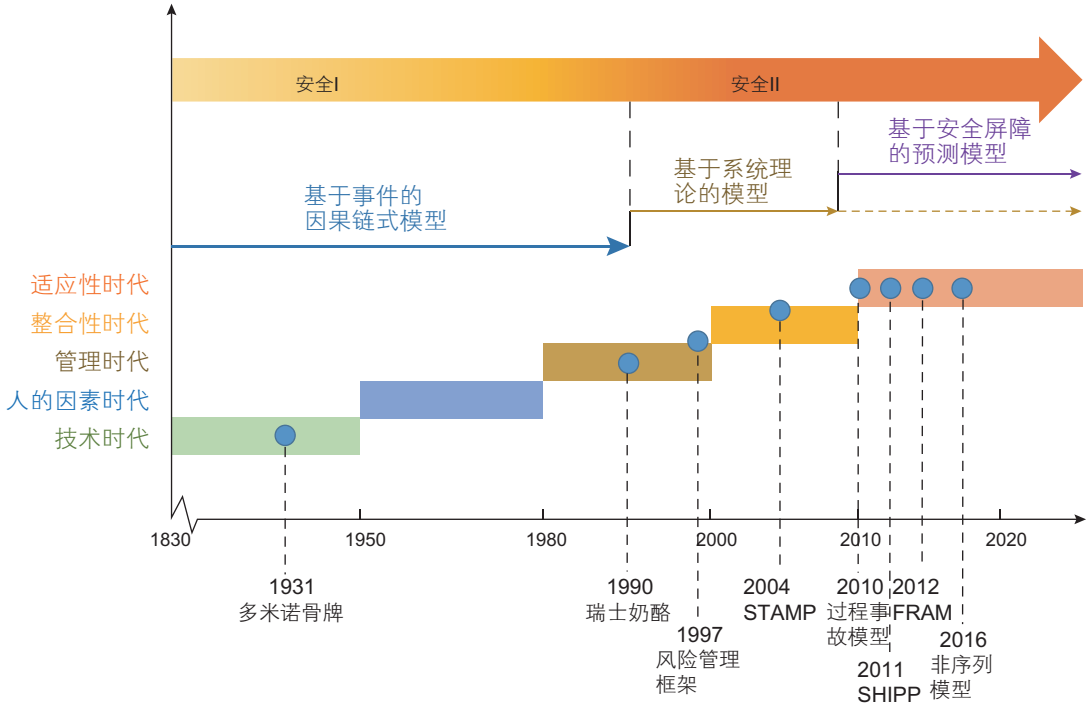

图 1 安全思维和事故模型发展历程

Fig. 1 The development of safety thinking and accident models

2 基于事件的因果链式模型

2.1 简单线性模型

事故模型反映人们思考安全的方式，并极大地影响识别和控制危害以及预防事故的能力。早期工业事故预防的重点是不安全条件，例如打开的刀片和未受保护的传送带。随着最明显的危害被消除，不安全条件减少的程度开始放缓，安全防护的重点又转移到了不安全行为。1919 年提出的事故频发倾向论是最早的解释工业事故的理论之一，该理论将工厂中具有某些性格特征的少数工人视为事故频发的主要原因[28,29]。该理论虽然指出人类潜在的不可靠性，但并没有明确描述事故的发生方式，并不是一个正式的模型。第一次明确指出人为差错的事故模型是海因里希的多米诺骨牌模型[12]。如图 2 所示，与事故有关的因素被表示成遗传和社会环境、人的过错、不安全行为和条件、事故和伤害这 5 个多米诺骨牌，第一个骨牌倒塌会相继击倒后面的骨牌直到伤害发生，同样地，如果移去其中一个骨牌，事故过程就被中止。海因里希将事故解释为一系列按特定时间顺序离散事件相继发生的结果，即伤害是事故的结果，事故仅由人的不安全行为或物的不安全条件直接造成，而不安全行为和条件的产生是由人的过失导致的，人的过失是由环境造成的或由遗传继承而来。

由于多米诺骨牌模型过分简化了事故中人类行为控制的过程，Bird[30–31] Adams[32–33] 和 Weaver[33–34] 等人又在此基础上扩展了基本的多米诺模型，将管理决策纳入事故因素。尽管如此，这一类简单线性事故模型被普遍认为过于简单，在日益发展的复杂社会技术系统中已经不再适用。

2.2 复杂线性模型

由于对更合理的事故理解方法和更强有力的事故模型的需求，简单线性模型在 20 世纪 80 年代被流行病学模型所替代。流行病学模型将导致事故的事件类比为疾病的传播，认为事故是偶然同时存在于空间和时间中的多种因素作用的结果[5]。最著名的流行病学模型是 Reason 提出的瑞士奶酪模型[13,35]。如图 3 所示，Reason 认为在不安全条件和最终损失之间存在多层防御系统，即由箭头尖端的“不安全行为”切片和影响不安全行为的一系列潜在条件组合而成。每个切片上的“洞”代表了各层防御系统的脆弱性，当不安全条件依次突破所有防御层的“洞”，则事故发生。瑞士奶酪模型对于事故分析和调查非常有用，它迫使调查人员关注不安全行为以外的潜在失效原因，便于发掘系统所存在的更深层次和更关键的脆弱模式。然而，该模型并没有关于奶酪上“洞”的确切定义，其抽象性阻碍了模型的实际应用[36]。为了便于事故的调查和分析，Wiegmann 和 Shappell 在瑞士奶酪模型的基础上建立了人的因素分析与分类系统 (HFACS，Human Factors Analysis and Classification System)，对奶酪上的“洞”进行了明确定义[36–39]。由于该分类系统的因素是基于数百例飞行事故总结提炼出的，HFACS 框架被各领域学者广泛采用。但 HFACS 框架主要涉及人的因素的分类，没有强调与设备设计等有关的技术性因素，且过分简化了发现系统“漏洞”到修复“漏洞”

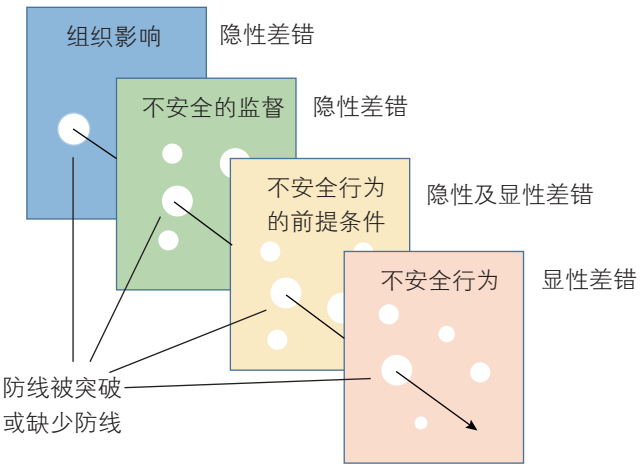

图 3 瑞士奶酪模型

Fig. 3 Swiss cheese model of accident causation

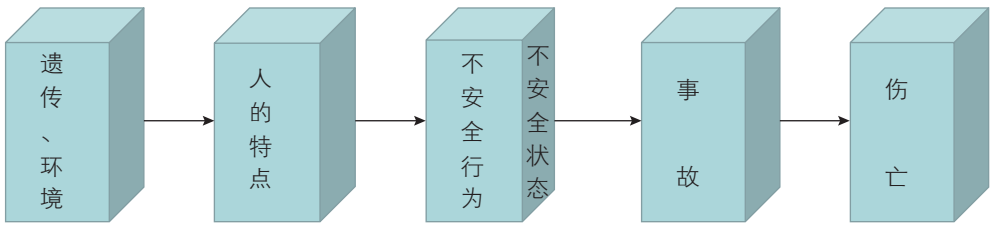

图 2 多米诺骨牌模型

Fig. 2 The Domino model of accident causation

的过程，这在一定程度上限制了它的应用范围。

尽管流行病学模型相对简单线性模型对事故的发生方式进行了更复杂的设计，但它仍然遵循线性因果模型的原理[40]，即人的失效和隐性条件的组合引发不利结果。此外，各防御层顺序失效的模式简化了各系统组件间复杂的交互关系[41]，且对瑞士奶酪模型过分规范性的应用可能导致将事故完全归因于高级管理人员而忽略一线人员的贡献[42]。

基于事件的因果链式模型对于工程设计安全性以及安全分析人员调查事故都具有重要意义，因为如果事故是由一系列事件引发，那么最明显的预防措施就是在损失发生之前将其中断。虽然事故的结果是由一系列原因造成的，但并不意味着通过结果能够推论出相同的原因[9]。正如Leveson教授[43]所说，事故成因和结果的关系就好比吸烟和肺癌的关系，许多吸烟者没有患上肺癌，而有些患有肺癌的人也不是吸烟者。过去和未来并不总是对称的，未来的事故并不总能重复与过去相同的事故模式。因此，无论是简单线性模型还是复杂线性模型都不足以对现代社会技术系统中多因素存在方式和因果演变模式作出全面的解释。

3 基于系统理论的事故模型

系统理论可以追溯到 20 世纪 30 年代，它是对传统分析技术局限性的回应，以应对当时开始建立的日益复杂的系统[44]。Wiener将这种思维应用于控制和通信工程[45]。Bertalanffy也提出了通用系统理论，认为各领域中的复杂系统都能基于通用系统理论表示成多层次模型系统[46]。传统分析方法基于分治法，将系统的物理部分和人类行为分别分解为单独的物理组件和离散事件，并假设每个组件或子系统都是独立运行的。系统方法则侧重于整个系统而不是单独的组件，充分考虑社会和技术层面的所有组成并研究各子系统间的相互作用[47]。具有代表性的基于系统理论的事故模型有Rasmussen的风险管理框架、STAMP模型和FRAM模型。

3.1 社会技术系统风险管理框架

工业系统是技术、社会和组织管理要素相互作用的社会技术系统。技术的日趋复杂和社会的快速发展使得工业系统不仅受内部系统波动的影响，同时也受市场竞争、经济和政治压力等动态环境条件的影响。动态环境中的风险管理不应再简单地基于对过去事故的响应，必须基于对实际的安全状态的观察或测量开发自适应的闭环反馈控制策略[48]。因此，Rasmussen[22,49]采用基于控制理论概念的面向系统的方法提出了社会技术系统风险管理框架，主要包括结构和动态两部分。

如图 4 所示，风险管理框架将复杂的社会技术系统描述为一个从立法者、组织和运营管理到系统操作的层次结构。系统各层级之间的相互依赖关系由动态工作流表示。成功的系统运转应该是有关高层控制的信息向下过滤到较低层，较低层的工作表现向上反馈到较高层。这种垂直的信息流形成了一个闭环反馈系统，并在整个社会技术系统的安全中起着至关重要的作用，它意味着事故是由各级决策者的决策和行动引起的，而不仅仅是过程控制级的工人引起的。

如图 4 的右侧所示，复杂的社会技术系统的各层级的行为受外部破坏力的影响，这些破坏力具有不可预测且快速变化的特点。系统的每个层级都在不同的时间承受不同的压力，为确保系统安全运行，重要的是确定安全操作的边界以及可能导致社会技术系统朝着或跨越这些边界迁移的动力。Rasmussen将动态工作环境中行为变化机制与热力学模型中边界条件和场梯度进行了类比。图 5 展示了可以影响复杂社会技术系统行为的动力，主要有个人无法接受的工作量、经济约束以及安全法规和程序。经济压力会产生成本效益梯度，从而影响个人采取更具经济效益的工作策略；工作量压力导致工作量梯度上升，从而促使个人改变工作方式以减少认知或体力劳动。这些适应性行为会在一段时间内导致人们越过安全工作法规的边界，并导致系统向可接受行为的边界迁移，如果越过边界则会导致事故发生。因此，改善风险管理最有前途的方法是明确安全操

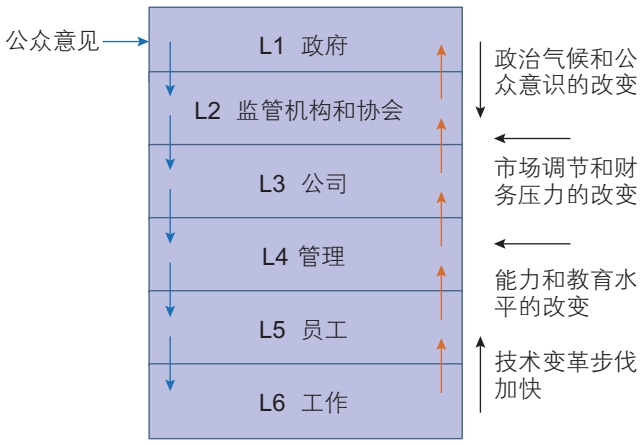

图 4 社会技术系统层次模型

Fig. 4 Hierarchical model of social-technical system

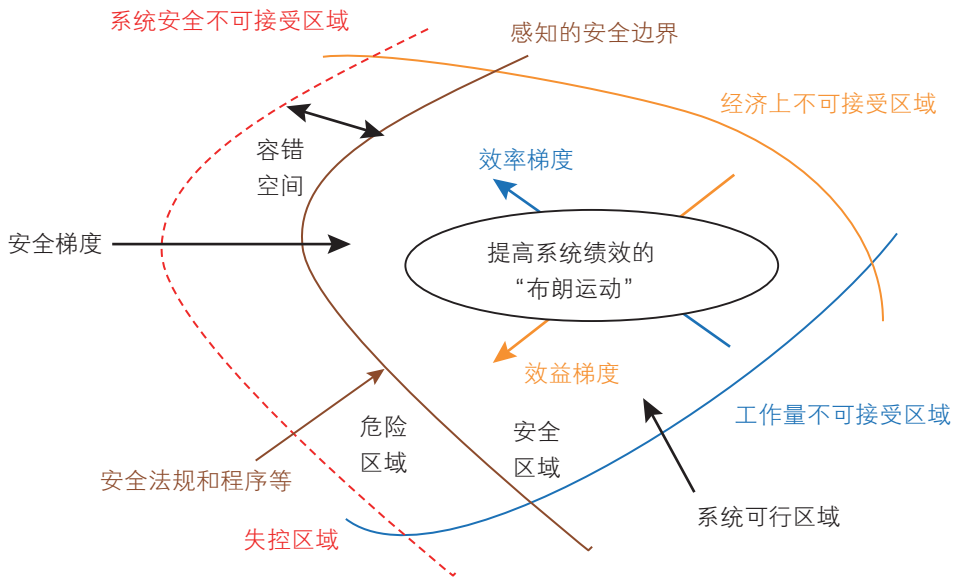

图 5　社会技术系统安全梯度和安全边界

Fig. 5　Safety gradients and boundaries of social-technical system

作的边界，并努力使参与者了解这些边界，并为他们提供学习应对边界的机会。

结合风险管理框架，Rasmussen开发了事故地图(Accimap, Accident Map)方法，以图示方式描述框架中考虑的 6 个系统层级的故障、决策、行动以及它们之间的相互作用。Rasmussen的风险管理框架及其描述性方法已在公共卫生[50−51]、石油化工[52]、太空旅行[53]和户外活动[54]等领域进行应用，这些案例研究验证了该框架对于事故解释的有效性。尽管如此，该框架模型缺乏对于安全边界的明确定义以及可用的原因分类体系，需要进一步研究以扩展该框架对于事故定量分析和预测的适用性。

3.2　STAMP模型

Leveson[23]遵循Rasmussen主动安全管理的思路，开发了STAMP模型从而使系统方法更加明确。根据Leveson的观点，安全性是系统的技术、物理、人和组织的组成部分相互作用时系统的涌现属性，当组件故障、外部环境干扰或系统组件之间不合适交互不受控制时就会发生事故[55]。因此，STAMP是基于约束的模型，重点关注系统组件和整个工作系统中所使用的控制机制之间的相互作用。

与Rasmussen的风险管理框架类似，STAMP模型中最核心的概念是层次结构，但STAMP模型所涉及的系统更加完整，因为它使系统开发和系统设计处于系统运行的前列[56]。如图 6 所示，STAMP将系统视为基于控制和约束的层次结构，结构中的每个层级都在下面较低层级上施加约束，而较低层级上有关控制和约束的适合性和条件的信息向上面的较高层级传递。STAMP强调复杂系统是基于物理、社会和经济压力动态地向事故迁移，而不是突然失去控制能力。发生系统事故的原因不是组件失效，而是因为未能成功实施约束，使系统更接近安全性能的边缘并降低安全运行的余地。约束限制了系统行为，确保其在安全范围内运行。约束既可以是现有的，例如环境或财政约束，也可以是引入的约束，例如规则，程序或设备或技术设计，它们代表对系统行为的控制，以限制组件之间的自由度[57]。由于已有的技术在适应更复杂社会技术系统的应用方面存在严重局限性，Leveson基于STAMP框架开发了基于系统理论的过程分析技术(STPA, System−Theoretic Process Analysis)和基于STAMP的因果分析技术(CAST, Causal Analysis based on STAMP)分别用于事故过程危害分析和事故因果关系分析[23,43,58]。

STAMP模型提出后获得了广泛关注，已成功应用于航天系统[59−60]、海运系统[61]、铁路系统[62−64]和石油化工[65−66]等领域。相比Accimap分析，STAMP能生成更可靠的事故分析结果并提供更全面的建议[67]，但STAMP更适合于对技术控制故障进行识别和分类，而不适合复杂的人为决策和组织失效[68−69]。因此，STAMP通常与HFACS等提供详细人因分类指南的方法结合使用。此外，STAMP无法提供事故过程的明确

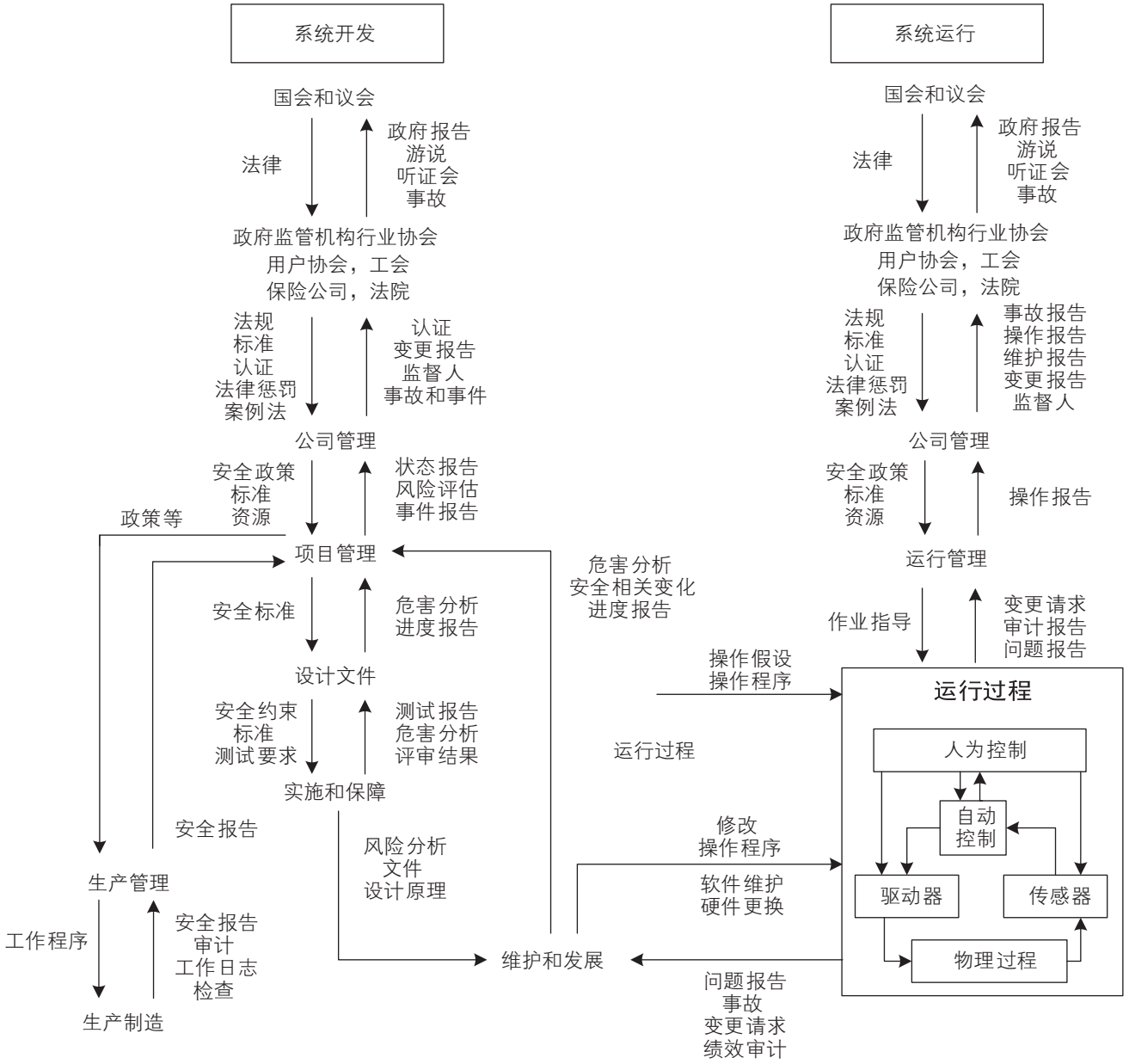

图 6 社会技术系统通用控制结构

Fig. 6 General control structure of social-technical system

图示，其内在的复杂性和难以操作使其难以被广大从业人员接受。

3.3 FRAM 模型

与 Rasmussen 和 Leveson 一样，Hollnagel 对基于线性因果理念解决安全问题的方法不满。他认为当前所有事故调查和风险评估都是在相对不了解系统完整行为的状态下进行的，且所有已建立的风险评估方法都要求有详细描述系统的方案，但所有的社会技术系统都是动态变化的，即使知道它们是什么，也无法完全定义或描述系统中的时空参数。因此，Hollnagel 基于安全 II[9] 和弹性复原力 [20] 概念提出了功能共振分析方法。从具体实施角度出发，FRAM 并不是表征系统行为的模型，而是一种方法。它可以识别和定义系统功能和可变性，并确定可变性如何以导致不良后果的方式在系统内相互作用。与 Rasmussen 的风险管理框架和 Leveson 的 STAMP 模型相比，FRAM 并不以分层或抽象的方式解释系统，而是以相对于整个系统的相互耦合或依赖功能来解释系统，重点是系统做什么而不是系统是什么 [70]。通过了解系统执行的功能，

可以在系统与其环境之间进行区分，从而确定系统边界。

在进行FRAM评估时，首先将系统分为直接或间接影响活动结果的关键功能。如图 7 所示，通过输入、输出、时间、控制、前提条件和资源 6 个基本参数表征系统的基本功能。然后在功能及其来源中定义潜在的可变性，即考虑正常和最坏情况下的差异。最后，通过观察到的功能之间的依存和耦合关系以及观察到的变异性来识别和描述功能共振，从而确定变异性的控制机制并指定所需的性能监控。

FRAM是揭示系统不同功能之间耦合和依赖关系的有效工具，已成功应用于航天系统[71−72]、海事系统[73−74]、核能系统[75]、石油化工[76]等领域。FRAM提供了一个事故分析框架，使复杂的人与技术交互关系更容易识别，并可以提供适当的监控策略和弹性设计方案以提高系统安全性[77]。但由于应用和分析过程不详细以及缺乏一致或明确的停止规则，FRAM中的功能识别和交互分析受到限制[78−79]。因此，需要进一步评估FRAM对于事故调查早期阶段中收集和组织数据的适用性，以及研究有关功能识别和屏障建立的更结构化的方法。

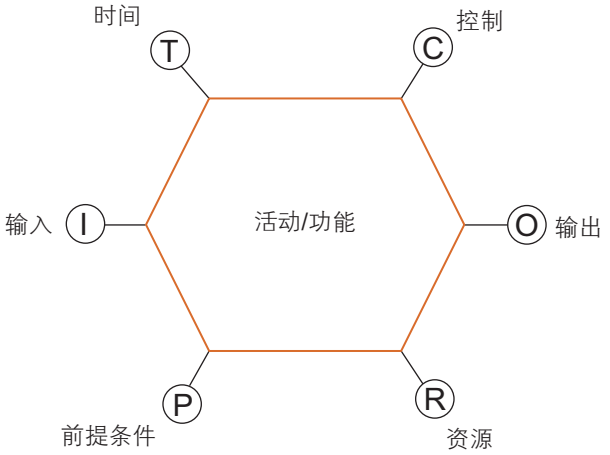

图 7　FRAM模型功能参数图

Fig. 7　Function parameters of FRAM model

除了上述 3 种模型，基于系统理论的事故模型还有Perrow[14,80]的正常事故理论(Normal Accident Theory)和Dekker[81]的漂移失效模型(Drift into Failure Model)。但这两种模型没有提供具体的方法论和操作步骤，实际应用中一般只是借鉴它们的内在理论。总体来说，基于系统理论的事故模型充分考虑了复杂系统内组件的非线性交互作用，并且以主动监控变异性代替被动事后分析，比基于事件的因果链式模型更先进合理。然而，这些模型大多不能直接应用于描述过程设施事故，并且建模方法通常应用于职业性伤害而非石油化工过程事故。此外，这些模型主要提供事故过程的定性描述，缺乏定量预测和评估。因此，更简洁便利、具有预测功能的基于安全屏障的事故预测模型出现在人们的视野中。

4　基于安全屏障的事故预测模型

安全屏障概念起源于能量转移观点。20 世纪 60 年代和 20 世纪 70 年代，Gibson和Haddon分别提出了两种开创性的安全理论以研究过剩能量从释放源到脆弱目标的过渡。1961 年，Gibson基于“能量转移超过身体伤害阈值会导致人身伤害”这一事实建立了能量模型[82]。1970 年，Haddon在该模型基础上将已知的事故预防原则系统化为十种策略[83]。1987 年，Kjellén将Haddon提出的事故预防策略定义为屏障[84]。之后，Reason于 1997 年基于纵深防御概念建立了如图 3 所示的瑞士奶酪模型。该模型提供了安全屏障概念性建模方法，后续的许多安全屏障模型都以此为基础。

4.1　过程事故模型

结合Reason的瑞士奶酪模型和Bird的因果链式模型的特征，Kujath等人[25]于 2010 年开发了针对海上石油天然气的过程事故模型。该模型假设海上油气设施中的事故由碳氢化合物释放引发，继而通过物质扩散和能量传递引发更严重的事故，而各级事故的中断

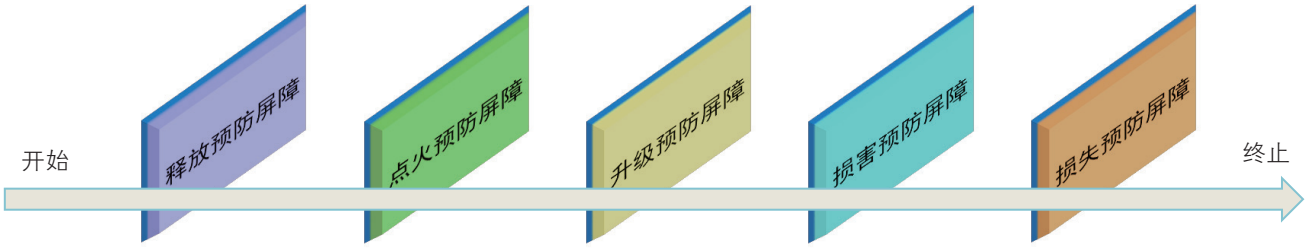

图 8　海上石油天然气过程事故模型

Fig. 8　Offshore oil and gas process accident model

和控制通过设置安全屏障实现。如图 8 所示，模型在事故传播路径上设置了 5 个防护屏障以预防或减轻物质或能量释放的影响，最坏的情况是所有屏障均失效导致重大或灾难性事故。对于模型所描述的事故过程，Kujath 等人进一步采用故障树和事件树相结合的方法分析具体事故。通过分析历史事故资料，挖掘并整理各安全屏障失效的影响因素，生成综合性的故障树模型；定义每个安全屏障失效后引发的事故类型，基于事件树方法分析不同严重程度事故的发生概率。该模型被成功应用于 1988 年派珀·阿尔法 (Piper Alpha) 事故和 2005 年德克萨斯州炼油厂事故中，但它仅将技术故障视为事故起因，并未考虑人的因素和组织错误等原因。

4.2 SHIPP 模型

为克服 Kujath 的过程事故模型的缺点，Rathnayaka 等人[26]建立了 SHIPP 模型，将适用范围从海上石油天然气扩展到了整个过程工业。如图 9 所示，在 SHIPP 框架内，与技术、人员、管理和组织方面有关的所有事故原因均被包括在内，并被归纳为 7 个预防屏障。其中释放预防屏障 (RPB，Release Prevention Barrier)、点火预防屏障 (IPB，Ignition Prevention Barrier) 和升级预防屏障 (EPB，Escalation Prevention Barrier) 与 Kujath 的过程事故模型相同，扩散预防屏障 (DPB，Dispersion Prevention Barrier)、人的因素预防屏障 (HFB，Human Factor Barrier) 以及管理和组织预防屏障 (M&OB，Management and Organizational Barrier) 是 SHIPP 模型独有的，损害控制和应急管理屏障 (DC & EMB，Damage Control and Emergency Management Barrier) 综合了 Kujath 的过程事故模型中的损失和损害预防屏障。Rathnayaka 将事故后果定义为安全偏离、未遂事故、轻微事故、一般性事故、重大事故和灾难性事故 6 个等级，通过 SHIPP 模型分析不同场景所对应的不同等级事故发生的可能性。SHIPP 模型保留了海上石油天然气过程事故模型中故障树和事件树相结合的系统分析方式，但是增加了贝叶斯更新机制分析企业实时安全数据以更新事故过程安全屏障的失效概率，从而最大程度地降低经验数据的不确定性。此外，SHIPP 还采用随机预测模型来计算下一个时间间隔内异常事件的数量。这些预测和故障更新功能可为企业的维护和变更管理提供决策支持，并有助于安全计划的优先级排序。

目前，SHIPP 模型已成功应用于液化天然气设施和钻井平台[85–87]，但该模型存在一定的局限[88]。一方面该模型未考虑外部因素和职业性伤害，且事故路径中的某些屏障不合逻辑；另一方面，事故数量预测技术对于嘈杂数据的灵敏性较差。尽管如此，SHIPP 仍然是一个非常受欢迎、功能强大的事故分析和预测工具。已有相关文献对 SHIPP 模型进行改进以更适应特定工作场所的分析[89–91]。

4.3 基于安全屏障的非序列模型

在 Rathnayaka 研究基础上，Adedigba 等人[27]进一步开发了基于安全屏障的非序列模型。该模型着眼于不同种类屏障的防护效应，并综合考虑了设计、设备、人员、管理和外部环境等因素之间的相互依赖性。如图 10 所示，设计错误可能导致操作和设备失效，操作失效可能会导致设备失效。3 种因素都可能直接引发事故，而它们又潜在地受人的因素、组织失效和外部因素的影响。与 SHIPP 模型类似，该模型仍然基于故

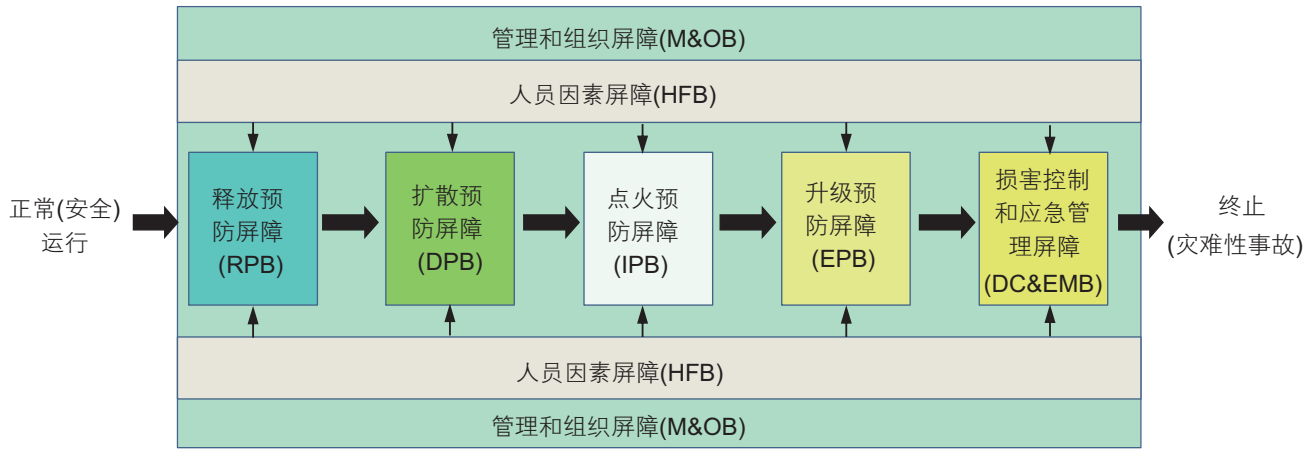

图 9 SHIPP 模型架构

Fig. 9 The architecture of SHIPP model

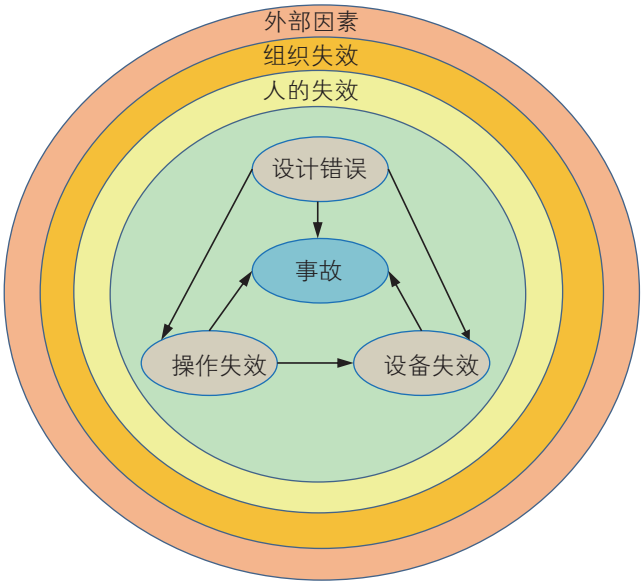

图 10　基于安全屏障的非序列模型

Fig. 10　Non-sequential barrier-based process accident model

障树和事件树来研究因果关系，但故障树被转换成贝叶斯网络从而能够考虑原因因素之间的非线性相互作用。该模型被应用于里士满炼油厂事故，通过在贝叶斯网络中使用OR、Noisy−OR和Leaky Noisy−OR这3种不同的逻辑门确定每个安全屏障失效概率的上下边界，从而得到事故发生概率的区间估计。该模型提供了一种基于影响因素的相互依赖性和非线性相互作用预测过程事故的机制，利用过程监控数据，该模型可以定量估计动态风险概况。但该模型缺乏各事故成因的具体分类指南，事故后果严重程度基于各影响因素屏障失效的数量判定，这种演变模式缺乏明确的证据。

总的来说，基于安全屏障的事故预测模型不仅能提供事故的定性描述和定量预测，而且通过事故过程与安全屏障的耦合能提供需监控的指标和预防性策略。事故预测模型兼具因果链式模型的简洁性思维和系统模型的系统性思维，建模方式更符合现场管理的实际需求。但由于过程事故发生和演变的复杂性，当前可用的事故预测模型无法提供所有事故类型的分析指南。此外，需要引入高灵敏度的预测方法来跟踪实时数据变化从而改进预测性能。

5　讨论与展望

从技术时代到适应性时代，安全管理经历了从基于事后响应的被动性思维向基于实时监控的主动性思维的过渡。在安全理论发展的过程中，研究者们致力于开发事故模型用于表征系统安全性的演变规律。事故模型依据不同的安全思维主要分为基于事件的因果链式模型、基于系统理论的事故模型以及基于安全屏障的事故预测模型。事故模型演变和发展过程中的相关安全理论的描述见本文附录。

5.1　三类事故模型的对比

基于事件的因果链式模型遵循线性思维，将事故视为一系列不期望事件相继失效的结果。以多米诺骨牌为代表的简单线性模型将事故视为单一原因的结果，识别并消除该单一原因则事故将不会重复发生。然而，现实情况是事故总是由多因素共同作用导致的，事件也不会如预期一样按特定顺序发生。因此，简单线性模型在当前日益复杂的社会技术系统中已经基本淘汰。流行病学模型以更复杂的方式描述事故，将事故成因细化为显性失效和隐性失效，显性失效直接引发不良的后果，而隐性失效又为显性失效创造了时空条件。流行病学模型本质上仍然遵循线性思维模式，显性因素和潜在因素的组合引发最终结果。尽管如此，流行病学模型提供了事故预测和预防一体化的思想，为后面更完善的安全屏障模型奠定了基础。

基于系统理论的事故模型在主动性安全管理的需求中应运而生，不再关注系统为什么失效，更关注系统怎样失效。通过建立系统各层次之间的控制和反馈关系监控系统的变异性，使理想的安全性和实际的安全性趋于一致。风险管理框架提供了社会技术系统的层级划分，各层级通过控制和反馈形成垂直的信息流闭环系统，阻止系统在外部动态破坏力的作用下向安全边界迁移。在风险管理框架下，Accimap技术被开发用于将事故的影响因素映射到复杂社会技术系统各层次中，分析各影响因素间的交互关系和安全性的变化过程。STAMP模型对社会技术系统的分层进行了细化和完善，描述了系统开发和设计如何与系统操作和运转相互作用和促进。STAMP模型非常有助于分析人员探究可能导致性能下降和不期望事件的系统组件之间的复杂交互，是基于系统理论的事故模型中应用最广泛的模型。但该模型由于分析过程复杂且缺乏简单明晰的图表输出，因此并不适合一般从业人员使用。FRAM模型认为事故是正常性能变异的意外组合导致的，风险管理的目标是确定并减少变异性，以阻止系统状态共振情况的发生。该模型提供了识别系统变异性以及确定变异性在系统内相互作用模式的方法，但对于如何调查事故和确定功能共振并未给出详细的指南。基于系统理论的事故模型从系统复杂性出发，表征系统不同层次的动态非线性交互过程，其所蕴含的

安全变异过程和方式更接近实际情况。但这一类模型更多关注安全性如何变化，缺乏适用于现场分析人员的可用性指南和合适的风险量化技术。后续的发展应结合事故先兆指标，提供对于事故因果关系的定量分析和综合性预测方法。

基于安全屏障的事故预测模型综合了线性模型和系统模型的优点，既综合考虑了系统组件间复杂的耦合关系，又保留了更符合现场人员思维模式的事件驱动理念。此类模型基于能量释放和控制的观点，充分考虑事故发生和演变特征，将安全屏障的预防和减缓效应融入事故过程，能够实现对于事故的预测和预防，因此非常适合过程工业的安全分析。目前，SHIPP模型是此类模型中最受欢迎和最有前途的模型，它阐述了事故从初始释放到逐渐恶化再到灾难性后果的演化过程，并提供了如何利用实时安全数据进行安全状态预测的详细方法。但该模型仍然是不完善的，因为它并未包括过程工业所有类型事故，也未综合考虑外部因素和其他类型因素，而且并未提供对于有关技术、人员和组织等因素的具体分类指南。基于安全屏障的非序列模型虽综合考虑了更多因素以及因素间的相互作用，但并未提供交互关系的依据以及图示化描述相关交互如何导致不同后果恶化的过程。后续有关事故预测模型研究的趋势是以SHIPP模型为基础，但需进一步明确定义和总结不同类型的安全屏障，建立综合考虑所有事故类型的过程模型，并引入更高灵敏度的预测方法提高预测的准确性和鲁棒性。

5.2 事故模型研究展望

现有的事故模型都有其自身的功能和局限性，它们都有各自的应用范围和适合领域。线性模型虽然已经不适用于复杂系统，但事件驱动的思想仍然值得借鉴，这符合分析人员的简化假设和因果逻辑思维，并且它所催生的诸如故障树和事件树等实用的事故分析方法一直沿用至今。系统事故模型由于更真实地反映了系统组件的动态交互，几乎适用于所有领域，但用于不同领域时需要根据领域特点进行相应改进和引入相关分类框架和定量手段。基于安全屏障的事故预测模型由于充分考虑了能量和屏障的关系，具有再现事故发生和演变过程的功能，因此更适用于过程事故的分析。分析人员在分析具体问题时需要结合所研究问题的特点进行事故的筛选和改进。未来事故模型的发展趋势可能是不同模型之间的结合，也可能是全新的模型，但无论通过哪种方式构建模型，模型中的元素交互关系都应遵循动态非线性的特征。

6 结论

(1)基于事件的因果链式模型本质上遵循线性思维，即事故由单因素导致或由显性因素和隐性因素的组合导致，且通过逆向因果推断能够完全还原事故过程。由于过分简化事故因果关系，此类模型基本已经不适用于复杂社会技术系统。

(2)基于系统理论的事故模型采用控制论思想描述复杂系统组件间的非线性交互，重点关注系统组件表现和控制机制之间的相互作用，识别系统可能出现的变异性并阻止系统向安全边界迁移。需要进一步研究故障因素分类指南和引入量化方法增加该模型的实用性。

(3)基于安全屏障的事故预测模型以能量转移论为基础，综合了线性模型的事件驱动观点和系统模型的非线性交互观点，并提供了安全状态的动态预测方法，更适用于过程工业事故。需要进一步构建全面概述事故发生方式的图示模型并引入更可靠的预测方法以提供更明确有效的事故预测和预防指南。

(4)安全科学发展至今已步入适应性时代，安全管理思维也已从基于事后响应的被动式管理变为基于实时监控的主动式管理。未来事故模型的发展趋势是建立表征系统组件间动态非线性交互，并能基于安全指标和实时数据提供动态安全性预测的实用性模型。

参考文献

[1] 覃容, 彭冬芝. 事故致因理论探讨[J]. 华北科技学院学报, 2005(3): 7−16. [QIN R, PENG D Z. Discussion on accident-causing theories [J]. Journal of North China Institute of Science and Technology, 2005(3): 7−16.]

[2] 罗春红, 谢贤平. 事故致因理论的比较分析[J]. 中国安全生产科学技术, 2007(5): 112−116. [LUO C H, XIE X P. Comparison study of accident-causing theories[J]. Jounal of Safety Science and Technology, 2007(5): 112−116.]

[3] 陈宝智, 吴敏. 事故致因理论与安全理念[J]. 中国安全生产科学技术, 2008, 4(1): 42−46. [CHEN B Z, WU M. Etiologies of accident and safety theory [J]. Jounal of Safety Science and Technology, 2008, 4(1): 42−46.]

[4] 傅贵, 索晓, 贾清淞, 等. 10 种事故致因模型的对比研究[J]. 中国安全生产科学技术, 2018, 14(2): 58−63. [FU G, SUO X, JIA Q S,

et al. Comparative study of ten accident causation models [J]. Jounal of Safety Science and Technology, 2018, 14(2): 58−63.]

[5] QURESHI Z H. A review of accident modelling approaches for complex sociotechnical systems [C]. In: Proceedings of the Twelfth Australian Conference on Safety-Related Programmable Systems, Adelaide, Australia. 2007, pp. 47–59.

[6] FEYER A M, WILLIAMSON A(Eds.). Occupational injury: Risk prevention and intervention [M]. London: Taylor and Francis, 1998.

[7] GLENDON A I, CLARKE S G, MCKENNA, E F. Human safety and risk management (2nd edition.) [M]. Boca Raton, FL, 2006.

[8] BORYS D, ELSE D, LEGGETT S. The fifth age of safety: The adaptive age [J]. Journal of Health Services Research & Policy, 2009, 1(1): 19−27.

[9] HOLLNAGEL E. Safety-I and safety-II: The past and future of safety management [M]. Ashgate Publishing, Ltd., 2014.

[10] MANUELE, F A. On the practice of safety (4th edition.) [M]. John Wiley & Sons, Hoboken NJ, 2013

[11] FERRY T S. Modern accident investigation and analysis (2nd ededition.) [M]. New York: Wiley, 1988.

[12] HEINRICH H W, PETERSEN D, ROOS N R. Industrial accident prevention: A safety management approach (5th edition.) [M]. New York: McGraw-Hill, 1980.

[13] REASON J. Human error [M]. Cambridge, UK: Cambridge University Press, 1990.

[14] PERROW C. Normal accidents: Living with high-risk technologies [M]. New York: Basic Books, 1984.

[15] LEVESON N. System safety engineering: Back to the future [M]. MIT Aeronautics and Astronautics, Boston, 2002.

[16] HOLNAGEL E, WOODS D D, LEVESON N. Resilience engineeering: Concepts and precepts [M]. Aldershot, UK: Ashgate, 2006.

[17] TALEB N. The black swan: The impact of the highly improbable [M]. New York: Random House; 2007

[18] DEKKER S, CILLIERS P, HOFMEYR J H. The complexity of failure: Implications of complexity theory for safety investigations [J]. Safety Science, 2011, 49(6): 939−945.

[19] PATTERSON M, DEUTSCH E S. Safety-I, safety-II and resilience engineering [J]. Current Problems in Pediatric and Adolescent Health Care, 2015, 45(12): 382−389.

[20] HOLLNAGEL E, PARIES J, WOODS, D D, WREATHALL J. (Eds.). Resilience engineering in practice: A guidebook [M]. Farnham, UK: Ashgate, 2011.

[21] HOLLNAGEL E. The ETTO principle: Efficiency-thoroughness trade-off, why things that go right sometimes go wrong [M]. Ashgate, Farnham, Surrey, 2009.

[22] RASMUSSEN J. Risk management in a dynamic society: A modelling problem [J]. Safety Science, 1997, 27(2): 183−213.

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

[24] HOLLNAGEL E. FRAM: The functional resonance analysis method: Modelling complex socio-technical systems [M]. Ashgate Publishing Ltd, 2012.

[25] KUJATH M F, AMYOTTE P R, KHAN F I. A conceptual offshore oil and gas process accident model [J]. Journal of Loss Prevention in the Process Industries, 2010, 23(2): 323−330.

[26] RATHNAYAKA S, KHAN F, AMYOTTE P. SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description [J]. Process Safety and Environmental Protection, 2011, 89(3):151−164.

[27] ADEDIGBA SA, KHAN F, YANG M. Process accident model considering dependency among contributory factors [J]. Process Safety and Environmental Protection, 2016, 102: 633–47.

[28] 高景毅, 陈全, 孙旭红. 论事故频发倾向理论的适用性[J]. 中国安全生产科学技术, 2012, 08(7): 51−55. [GAO J Y, CHEN Q, SUN X H. Study on applicability of the accident proneness theory [J]. Journal of Safety Science and Technology, 2012, 08(7): 51−55.]

[29] 王凯全, 邵辉, 等. 事故理论与分析技术[M]. 北京: 化学工业出版社, 2004. [WANG K Q, SHAO H, et al. Accident theory and analysis technology [M]. Beijing: Chemical Industry Press, 2004.]

[30] STRANKS J W. Health and safety at work: Key terms [M]. Butterworth-Heinemann, Elsevier, 2012.

[31] RIDLEY J, CHANNING J. Safety at work (Seventh edition)[M]. Butterworth-Heinemann, Elsevier, 2012.

[32] CCPS. Guidelines for investigating chemical process incidents [M]. New York: America Institute of Chemical Engineers (AIChE), 2003.

[33] ABDELHAMID T S, EVERETT J G. Identifying root causes of construction accidents[J]. Journal of Construction Engineering and Management, 2000, 126(1): 52−60.

[34] TAYLOR G, EASTER K, HEGNEY R. Enhancing occupational safety and health [M]. Butterworth-Heinemann, Elsevier, 2004.

[35] REASON J. Managing the risks of organizational accidents[M]. Aldershot, Hants, Ashgate, 1997.

[36] WIEGMANN D, SHAPPELL S. A human error approach to aviation accident analysis: The human factors analysis and classification system[M]. Ashgate Publishing Ltd., Aldershot, 2003.

[37] SHAPPELL S A, WIEGMANN D A. A human error approach to accident investigation: The taxonomy of unsafe operations [J]. The International Journal of Aviation Psychology, 1997, 7(4): 269−291.

[38] SHAPPELL S A, WIEGMANN D A. Applying reason: The human factors analysis and classification system (HFACS) [J]. Human Factors and Aerospace Safety, 2001, 1(1): 59−86.

[39] WIEGMANN D, SHAPPELL S. A human error analysis of commercial aviation accidents using the human factors analysis and classification system (HFACS) [R]. Federal Aviation Administration Technical Report No. DOT/FAA/AM−01/3. National Technical Information Service, N Springfield, VA, 2001.

[40] HOLLNAGEL E. Barriers and accident prevention [M]. Hampshire, Ashgate, 2004.

[41] DEKKER S. The field guide to understanding human error [M]. Ashgate Publishing Limited, Aldershot, 2006.

[42] UNDERWOOD P, WATERSON P. Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models [J]. Accident Analysis & Prevention, 2014, 68: 75−94.

[43] LEVESON N. Engineering a safer world: Systems thinking applied to safety [M]. The MIT Press, London, 2011.

[44] CHECKLAND P. Systems thinking, systems practice [M]. New York: John Wiley & Sons, 1981.

[45] WIENER N. Cybernetics: Or the control and communication in the animal and the machine (2nd edition.) [M]. Cambridge, MA: MIT Press, 1965.

[46] BERTALANFFY L. General systems theory: Foundations [M]. New York: Braziller, 1969.

[47] ACKOFF R L. Towards a system of systems concepts [J]. Management Science, 1971, 17(11): 661−671.

[48] RASMUSSEN J, GOODSTEIN L P. Decision support in supervisory control of highrisk industrial systems [J]. Automatica, 1987, 23(5): 663−671.

[49] RASMUSSEN J, SVEDUNG I. Proactive risk management in a dynamic society [M]. Swedish Rescue Services Agency, 2000.

[50] WOO D M, VICENTE K J. Sociotechnical systems, risk management, and public health: Comparing the North Battleford and Walkerton outbreaks [J]. Reliability Engineering & System Safety, 2003, 80(3): 253−269.

[51] VICENTE K J, CHRISTOFFERSEN K. The Walkerton E. Coli outbreak: A test of Rasmussen's framework for risk management in a dynamic society [J]. Theoretical Issues in Ergonomics Science, 2006, 7(2): 93−112.

[52] GOODE N, SALMON P M, LENNÉ, MICHAEL G, et al. Systems thinking applied to safety during manual handling tasks in the transport and storage industry[J]. Accident Analysis & Prevention, 2014, 68: 181−191.

[53] JOHNSON C W, MUNIZ DE ALMEIDA I. An investigation into the loss of the Brazilian space programme's launch vehicle VLS−1 V03 [J]. Safety Science, 2008, 46(1): 38−53.

[54] SALMON P, WILLIAMSON A, LENNE M, et al. Systems-based accident analysis in the led outdoor activity domain: Application and evaluation of a risk management framework [J]. Ergonomics, 2010, 53(8): 927−939.

[55] LEVESON N. The need for new paradigms in safety engineering [C]. In: Safety− Critical Systems: Problems, Process and Practice (2009): 3–20. Proceedings of the Seventeenth Safety-Critical Systems Symposium, Brighton, UK, 3–5 February 2009.

[56] PASMAN H J. Risk analysis and control for industrial processes – gas, oil and chemicals: A system perspective for assessing and avoiding low-probability, high-consequence events [M]. Elsevier Science, 2015.

[57] DEKKER S. The field guide to understanding 'human error' [M]. Ashgate Publishing, Ltd, 2014.

[58] LEVESON N. Rasmussen's legacy: A paradigm change in engineering for safety [J]. Applied Ergonomics, 2017, 59(Part B): 581−591.

[59] JOHNSON C W, HOLLOWAY C M. The ESA/NASA SOHO mission interruption: Using the STAMP accident analysis technique for a software related 'mishap' [J]. Software Practice & Experience, 2003, 33(12): 1177−1198.

[60] LU Y, ZHANG S G, TANG P, et al. STAMP-based safety control approach for flight testing of a low-cost unmanned subscale blended-wing-body demonstrator [J]. Safety Science, 2015, 74: 102−113.

[61] KIM T, NAZIR S, ØVERGÅRD K I. A STAMP-based causal analysis of the Korean Sewol ferry accident [J]. Safety Science. 2016, 83: 93–101.

[62] OUYANG M, HONG L, YU M H , et al. STAMP-based analysis on the railway accident and accident spreading: Taking the China–Jiaoji railway accident for example [J]. Safety Science, 2010, 48(5): 544−555.

[63] 肖宁. 基于系统理论的铁路系统多事故致因共性研究[D]. 华中科技大学, 2013. [XIAO N. System Theory-based common causation analysis of multiple accidents on the railway system [D]. Huazhong University of Science and Technology, 2013.]

[64] 闫宏伟. 基于STAMP的轨道交通全自动运行系统安全分析研究[D]. 北京交通大学, 2016. [YAN H W. Safety analysis of fully automatic operation system of rail transit based on STAMP [D]. Beijing Jiaotong University, 2016.]

[65] MENG X, CHEN G, SHI J, et al. STAMP-based analysis of deepwater well control safety [J]. Journal of Loss Prevention in the Process Industries, 2018, 55:41−52.

[66] OUEIDAT D, GUARNIERI F, GARBOLINO E, et al. Evaluating the safety operations procedures of an LPG storage and distribution plant with STAMP [J]. Procedia Engineering, 2015, 128: 83−92.

[67] FILHO A, JUN G, WATERSON P. Four studies, two methods, one accident –An examination of the reliability and validity of accimap and STAMP for accident analysis [J]. Safety Science, 2019, 113: 310–317.

[68] SALMON P M, CORNELISSEN M, TROTTER M J. Systems-based accident analysis methods: A comparison of accimap, HFACS, and STAMP [J]. Safety Science, 2012, 50(4): 1158−1170.

[69] LI C, TANG T, CHATZIMICHAILIDOU M M, et al. A hybrid human and organisational analysis method for railway accidents based on STAMP-HFACS and human information processing [J]. Applied Ergonomics, 2019, 79: 122–42.

[70] LUNDBERG J, ROLLENHAGEN C, HOLLNAGEL E. What-You-Look-For-Is-What-You-Find—The consequences of underlying accident models in eight accident investigation manuals [J]. Safety Science, 2009, 47(10): 1297−1311.

[71] CARVALHO P V R D. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some character−istics of the air traffic management system resilience [J]. Reliability Engineering & System Safety, 2011, 96(11):1482−1498.

[72] HERRERA I A, WOLTJER R. Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis [J]. Reliability Engineering & System Safety, 2010, 95(12): 1269–75.

[73] PRAETORIUS G, HOLLNAGEL E, DAHLMAN J. Modelling vessel traffic service to understand resilience in everyday operations [J]. Reliability Engineering & System Safety, 2015, 141: 10–21.

[74] LEE J, CHUNG H. A new methodology for accident analysis with human and system interaction based on FRAM: Case studies in maritime domain [J]. Safety Science, 2018, 109: 57−66.

[75] LUNDBLAD K, SPEZIALI J, WOLTJER R, et al. FRAM as a risk assessment method for nuclear fuel transportation [C]. In: Proceed−ings of the international confererence working on safety, 2008.

[76] AGUILERA M V C, FONSECA B B D, FERRIS T K, et al. Modelling performance variabilities in oil spill response to improve system resilience [J]. Journal of Loss Prevention in the Process Industries, 2016, 41: 18–30.

[77] SMITH D, VEITCH B, KHAN F, et al. Understanding industrial safety: Comparing fault tree, Bayesian network, and FRAM approaches [J]. Journal of Loss Prevention in the Process Industries, 2017, 45: 88−101.

[78] LI W, HE M, SUN Y, et al. A proactive operational risk identification and analysis framework based on the integration of ACAT and FRAM [J]. Reliability Engineering & System Safety, 2019, 186: 101–109.

[79] 王仲. 功能共振分析方法在事故分析中的改进应用[D]. 中国地质大学(北京), 2017. [WANG Z. Improving application of function resonance analysis method in accident analysis [D]. China University of Geosciences, Beijing, 2017.]

[80] PERROW C. Organizing to reduce the vulnerabilities of complexity [J]. Journal of Contingencies and Crisis Management, 1999, 7(3): 150−155.

[81] DEKKER S. Drift into failure: From hunting broken components to understanding complex systems [M]. Ashgate, U. K, 2011.

[82] RUNYAN C W. Introduction: Back to the future–revisiting Haddon's conceptualization of injury epidemiology and prevention[J]. Epidemiologic Reviews. 2003, 25(1): 60–64.

[83] JOHNSON, C W. Failure in safety-critical systems: A handbook of accident and incident reporting [M]. Glasgow, Scotland, University of Glasgow Press, 2003.

[84] KJELLÉN U. Prevention of accidents through experience feedback [M]. London: Taylor & Francis, 2000.

[85] RATHNAYAKA S, KHAN F, AMYOTTE P. SHIPP methodology: Predictive accident modeling approach. Part II. Validation with case study [J]. Process Safety & Environmental Protection, 2011, 89(2): 75−88.

[86] RATHNAYAKA S, KHAN F, AMYOTTE P. Accident modeling approach for safety assessment in an LNG processing facility [J]. Journal of Loss Prevention in the Process Industries, 2012, 25(2): 414−423.

[87] RATHNAYAKA S, KHAN F, AMAYOTTE P. Accident modeling and risk assessment framework for safety critical decision-making: Application to deepwater drilling operation [J]. Journal of Risk and Reliability. 2013, 227(1): 86–105.

[88] AL-SHANINI A, AHMAD A, KHAN F. Accident modelling and analysis in process industries [J]. Journal of Loss Prevention in the Process Industries, 2014, 32: 319−334.

[89] XUE L, FAN J, RAUSAND M, et al. A safety barrier-based accident model for off shore drilling blowouts [J]. Journal of Loss Preven−tion in the Process Industries, 2013, 26(1): 164−171.

[90] TAN Q, CHEN G, ZHANG L, et al. Dynamic accident modeling for high-sulfur natural gas gathering station [J]. Process Safety & Environmental Protection, 2014, 92(6): 565−576.

[91] BAKSH A A, KHAN F, GADAG V, et al. Network based approach for predictive accident modelling [J]. Safety Science, 2015, 80: 274−287.

(编辑　马桂霞)

附录 相关安全理论描述

安全I：安全I定义是不良后果数量尽可能少的条件水平，即确保事故或异常事件数量在合理可行的范围内尽可能少。

安全II：安全II是对安全I的补充，即确保事情日常工作尽可能正确，而不仅仅关注错误的事情。

弹性复原力：弹性复原力是组织(系统)维持或恢复动态稳定状态的内在能力，强调组织(系统)在变化和扰动之前、之时和之后适应和调整的能力，使组织(系统)不仅能够从重大事故和/或承受持续压力后复原，还能在预期和意外情况下维持所需的运行机制。

系统理论：系统理论包括理解组件(设备设施、技术、人员、组织和管理)之间复杂相互关系所必需的原理、模型和规章。在应用系统理论观点进行安全性建模中，系统不被视为静态设计，而是被视为通过信息和控制的反馈对自身及环境的变化不断调整并实现系统目标的动态过程。

正常事故理论：正常事故理论以“耦合”程度描述系统组件之间的关系，并定义了松散耦合和紧密耦合。松散耦合描述了相互依赖程度较小的组件之间的相互作用，紧密耦合则描述了高度相关的组件之间的相互作用。该理论认为在系统具有复杂交互作用和紧密耦合情况下，事故是不可避免的且应被视为正常现象。

漂移失效模型：漂移失效模型认为系统是以无法预见的方式逐渐发生变化，并会越过安全边界漂移到不安全性能状态。组织应该通过监控、分析和反馈不断反思系统安全变化方式，确保系统朝着长期稳定运转的最佳方向发展。

能量转移观点：能量转移观点认为事故的发生是由于能量失去控制而意外释放，且转移的能量超过目标的最大承受能力。通过设置屏障约束和限制能量可以预防事故或减缓事故的影响程度。