Risk Identification Model Based on System Theory and Its Implementation Technical Analysis

Hubo Zhang, Tiezhong Liu

School of Management and Economics, Beijing Institute of Technology, Beijing 100081, China

基于系统理论的风险识别模型及其实现技术分析

张湖波，刘铁忠

北京理工大学管理与经济学院，北京 100081，中国

Abstract

In view of the interactive and systematic problems of accident caused by high technology, the method of risk identification in the perspective of system theory is studied. We analyze the Systems-Theoretic Accident Model and Process (STAMP) and the basic steps of Hazard Analysis Technology (STPA) based on STAMP, and use the STPA method to do empirical analysis on the causes of traffic accidents. Thereinto STAMP is based on the system theory and takes security constraints as the core. Theoretical and applied analysis results show that, STPA can identify risk systematicly, modularly and accurately compared with the traditional risk identification methods. Study of. STAMP and STPA can enrich the risk identification method and improve the ability of risk identification on complex system of high technology.

Keywords: Systems-Theoretic Accident Model and Process(STAMP);STPA Hazard Analysis Technology; risk identification; traffic accidents

摘要

针对高新技术条件下事故致因的交互性、系统性问题，开展了系统理论视角下的风险识别方法研究。理论分析了基于系统理论、以“安全约束”为核心的系统理论事故模型和过程（STAMP）及以此为基础形成的 STPA 风险识别方法的基本步骤，并使用 STPA 方法对道路交通事故原因进行了实证分析。理论分析与应用分析结果显示，与传统风险识别方法相比，STPA 能够系统化、模块化的准确识别风险。STAMP 理论和 STPA 技术对丰富风险识别方法，提高对高新技术复杂系统的风险识别能力有重要意义。

关键词：系统理论事故模型和过程（STAMP）；STPA 危险分析技术；风险识别；道路交通事故

1. 引言

风险识别是风险管理的一个重要环节，有效识别相关风险是后续风险分析的基础。传统事故致因理论分析方法，如故障树分析（FTA）、失效模式影响分析（FMEA）等一般通过事件链搜寻导致损失的原因来确定故障组件和故障模式，并依据基础事件的概率对系统进行概率安全分析[1]-[4]。这种将事故和原因之间的关系简单线性化的风险识别方法在传统安全领域是比较有效的[5]。但是，随着技术的发展，各组件之间已表现出越来越多的交互影响，尤其是社会与技术因素叠加使得事故致因更加复杂[6]，因此，以系统理论视角识别故障模式变得十分重要。

美国麻省理工大学航空航天软件工程研究实验室 Leveson 教授于 2004 年[7]针对复杂系统安全分析的需求从系统理论视角提出了系统理论事故模型和过程 STAMP（Systems-Theoretic Accident Model and Process）以及基于 STAMP 的风险分析技术

STPA（STAMP-Based Hazard Analysis）[8]。STAMP 模型及 STPA 技术最早应用于航空航天、核安全等高新技术领域，如 Nelson（2008）使用 STAMP 模型及 STPA 方法有效分析了 Comair 航空 5191 航班事故的原因，并进一步发现了航班飞行存在的安全隐患[9]；Yao Song 等（2012）人使用 STPA 技术从不同的系统层级分析了核安全问题，其实证结果表明 STPA 技术十分适合对复杂系统的安全性分析[10]；Altabbakh 等（2014）使用 STAMP 模型识别了油气工厂的风险，认为 STAMP 模型可以从不同系统层级发现直接和间接的不安全因素[11]。国内关于 STAMP 模型的相关研究较少，且大部分停留在片段式的理论介绍或简单的应用展示上，如阳小华等（2014）介绍了 STAMP 模型的基本概念，简单分析了核电厂蒸汽发生器(SG)水位控制系统的安全性问题[12]；李娟等（2010）使用 STAMP 模型分析了舰载作战系统软件的安全性，表明 STAMP 模型在研究设计阶段就能发现安全风险[13]；刘金涛（2015）综合使用 STPA 和其他方法分析了高速列车安全控制系统的有效性，发现 STPA 技术可与其他风险分析技术较好结合使用[14]。STAMP 模型及 STPA 技术已在一些高新技术得到了应用，但对其研究不够系统化，且大部分应用分析都针对高新技术领域，非专业人员受困于专业知识限制对 STAMP 模型及 STPA 技术的本质和使用认识会有偏差，对模型方法的理解推广不利。

本文将系统研究 STAMP 模型和 STPA 技术的理论来源、基本概念和逻辑结构，通过分析道路交通事故检验相关模型方法的有效性并具体展示 STPA 技术的操作过程。本文探讨的 STAMP 理论和 STPA 技术对丰富风险识别方法，提高对高新技术复杂系统的风险识别能力有重要意义。

2 理论分析

2.1 STAMP 模型

STAMP 模型是系统理论事故模型和过程英文名称 Systems-Theoretic Accident Model and Process 的缩写，是一种基于系统理论、以“安全约束”为核心的事故风险识别方法[15]。STAMP 模型的提出，基于技术的快速进步和新型危险的出现使得传统风险管理的一些条件发生了变化，尤其是在高新技术和系统工程领域原先风险管理的一些基本假设必须得到修正。表 1 列出了原假设及其修正。

表 1 风险分析的基本假设比较

原假设	新假设
系统或组件可靠性越强越安全；如果组件不失效，则事故不会发生。	高可靠性既不足以完全解决问题，也不是绝对必要。
事故是由相关的事件链引起的。我们可以通过分析事件链来理解事故和进行风险评估。	事故是一个包括社会-技术系统的复杂过程。传统的事件链不能对其进行完备的分析。
基于事件链的风险概率分析是评估风险的最好方法。	风险评估不应只包括简单的概率分析。
大多数事故是由人因错误引起的。利用奖惩制度可以减少事故发生。	人因错误植根于工作环境。为了减少操作者的错误，我们必须要改善工作环境。
高可靠性的软件是安全的。	高可靠性的软件不一定安全。
大部分事故是由许多随机事件的同时发生造成的。	系统有向高风险状态迁移的趋势。这种迁移是可预测的，通过恰当的系统设计和操作监督可以避免。
明确事故责任对防止事故发生是必须的。	责备是安全的敌人。应把精力集中于对整个系统行为的理解，而不是把责任分配给谁。

正是基于以上假设的改变，STAMP 模型认为风险识别应以系统理论为基础，兼顾社会原因与技术原因两个方面，将系统安全性视为复杂系统的涌现性。认为安全是一个控制问题，其最基本的概念是“安全约束”，系统的控制被认为是安全约束的执行。因此，事故的发生

是因为系统在设计、开发和运行过程等系统生命周期内违背了已有安全约束或已有安全约束无效。STAMP 逻辑结构如图 1 所示：

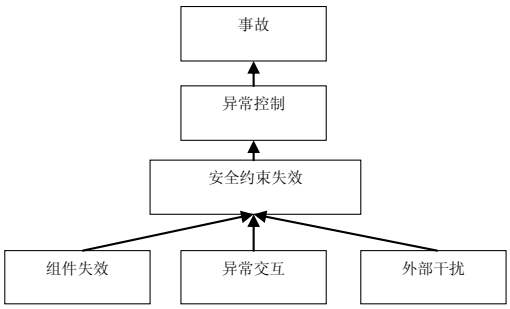

图 1　STAMP 逻辑结构图

STAMP 模型中有三个基本概念，分别是安全约束，分层控制结构及过程模型。下面进行相关分析：

第一，安全约束。安全约束是 STAMP 模型中最基本的概念，正是由于安全约束设计不足或没有得到正确的实施导致了事故的发生。安全约束包括积极的安全约束和消极的安全约束，积极的安全约束即通过采取各项主动措施确保安全，如各种监测系统；消极的安全约束即通过运用各种物理原理实现系统的自我防护，如自锁。为保障系统安全应尽量采用消极的安全约束。

第二，分层控制结构。系统论中用分层控制结构描述复杂系统，即将系统分为不同层次的控制过程，上一层的组织或结构通过控制过程来向下一层的组织或结构施加约束，同时下一层通过反馈向上一层反映安全约束的执行情况。事故发生是由上层结构对下层结构控制的无效（①通信失效：控制指令未得到有效传递；②执行器操作不当：控制指令执行错误；③延迟：控制指令未及时传递或执行；）或下层结构向上层结构反馈的无效（①没有反馈渠道；②通信失效：反馈信息未得到有效传递；③延迟：未及时反馈信息；④传感器操作不当：反馈信息不正确或没有提供反馈信息）引起的。STAMP 通过分层控制结构来分析系统中不同层次的控制过程，利用控制与反馈过程反映系统各部分的交互作用，为寻找更深层次的失效原因提供可能[16]。

第三，过程模型。过程模型是控制器对被控过程的理解和认知。过程模型可繁可简，但一般都要包括控制法则，系统当前状态和改变状态的方法过程，图 2 给出了基本的过程模型。过程模型通过反馈和控制过程的有效交互实现系统的正常运行，当控制过程与被控制过程不匹配时即有可能发生事故。控制过程与被控制过程不匹配的原因有：缺少必要的安全控制；采用了不安全的控制；过早或过晚地开始了安全控制；过早或过晚地结束了安全控制[5]。

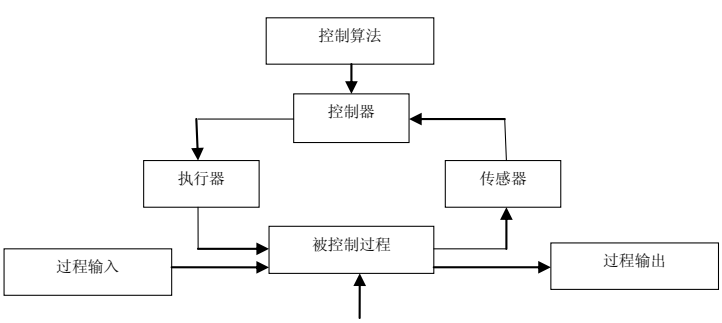

图 2　基本过程模型

2.2 STPA 方法

Leveson（2004）在 STAMP 模型的基础上提出了 STPA 这种系统理论过程分析方法。STPA 是一种自上而下的风险识别方法[17]。STPA 方法的主要步骤是针对界定的被分析系统，通过定义其系统级危险确定应有的安全约束，在此基础上分析系统安全约束的分层控制结构，辨识分层控制结构中可能出现的不安全控制（不能，过早或过晚的控制），最后确定不安全控制的产生原因。各阶段分析的主要关注点在 STAMP 模型中均已有描述[7]。

STPA 方法的具体过程如图 3 所示

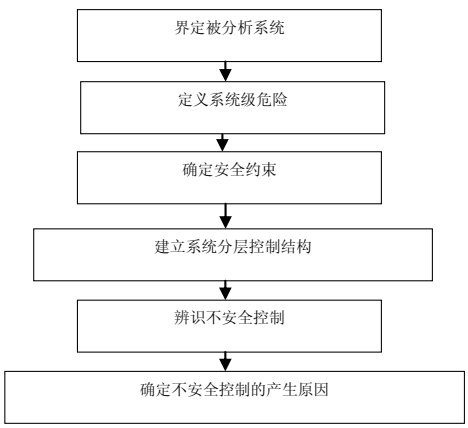

图 3　STPA 基本分析步骤

2.3 STAMP 与 STPA 主要特点

STAMP 模型从系统理论角度识别、解释风险，根据需要将分析对象分为不同的系统级别（模块）并逐层分析，不论系统级别大小均考虑组件失效（可靠性）、交互影响（同一模块内和不同模块间）和外界影响（技术、社会）等造成的安全约束失效对研究对象安全的影响，是一种综合考虑技术、社会因素的系统化的风险识别模型。STPA 技术是 STAMP 模型的具体化实现手段，通过由上而下、由整体到局部的逐级分解细化发现各层级可能存在的安全风险，为风险识别提供了标准化的操作流程。

3 应用分析

3.1 STPA 分析步骤

按照《生产安全事故报告和调查处理条例》（国务院令第 493 号）的规定，一次性死亡 3 人以上的道路交通事故需由市级以上政府部门进行调查并出具调查报告。根据上述标准，本研究共收集近 5 年发生的 108 个相关案例，分析后发现事故类型主要涵盖坠落（23.1%）、侧翻（19.4%）、相撞（43.6%）、追尾（13.9%）等四种，而事故调查原因一般有“驾驶员因素（超速、超载、非法驾驶（疲劳驾驶、酒驾、毒驾）、不安全操作行为（不安全超车、逆向行驶等））、车辆问题、道路环境问题、管控措施问题”等方面。

由此，本研究将使用 STPA 方法分析道路交通事故的原因，具体步骤包括：

第一，界定系统范围：分析由驾驶员、车辆、道路环境和管控措施构成的道路行车系统。

第二，定义系统级危险：汽车没有安全行驶，发生事故，造成人员伤亡。

第三，系统安全约束：驾驶员安全操作，车辆技术要求达标，道路环境良好，检查管理措施有效。所以，每个分析模块均由驾驶员因素、车辆因素、道路环境因素、检查管理因素构成。

第四，建立分层控制结构：通过分析系统内存在的控制、反馈模式，确定如图 4 所示的分层控制结构，由此确定各模块间、模块内部组件之间可能存在的交互影响。

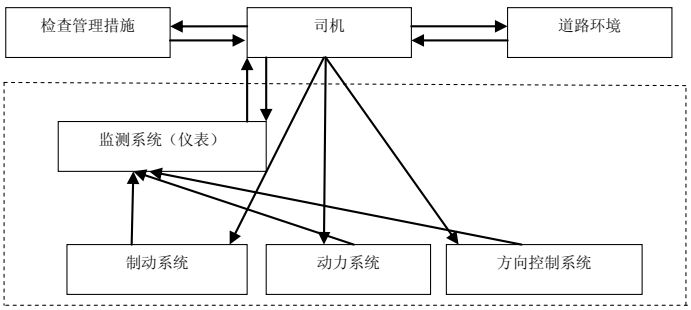

图 4　道路交通事故分层控制结构

第五，不安全的控制行为：根据案例分析结果发现道路交通事故发生的直接原因有超速、超载、没有按照安全合理路线行驶三类，分别对应表 1、表 2、表 3 三个分析模块。对应的细化的不安全控制行为有事故发生时没有减速、减速过慢、超载、逆向行驶、不安全超车、车辆冲出道路。

第六，不安全控制行为原因分析：控制缺陷分析基于控制和反馈两方面进行分析。针对已识别的不安全控制行为和已建立的分层控制结构对控制缺陷进行分析。

最终分析结果详见表 1-表 3。

表 1 超速原因

没有减速 a）驾驶员因素 控制：安全意识淡薄，有超速行驶习惯； 注意力不集中，没有发现情况或采取制动措施； 驾驶经验不足，没有采取有效制动措施 反馈：没有得到降速提示； b）车辆因素 控制：车辆制动系统故障，不能制动 反馈：车辆速度仪表盘显示不准确 c）道路环境因素 控制：道路条件较差（坡度过大、湿滑等）使车辆制动失效 反馈：视线条件较差使司机得不到减速信息 d）检查管理因素 反馈：没有减速行驶警示	减速过慢 a）驾驶员因素 控制：安全意识淡薄，有超速行驶习惯； 注意力不集中，不能及时发现情况或采取制动措施； 驾驶经验不足，没有及时采取有效制动措施 反馈：得到降速提示过晚 b）车辆因素 控制：车辆制动系统故障，制动能力不足 反馈：车辆速度仪表盘显示不准确 c）道路环境因素 控制：道路条件较差（坡度过大、湿滑等）使车辆制动能力不足 反馈：视线条件较差，司机得到减速信息太晚 d）检查管理因素 反馈：减速行驶警示设置不合理，不能有效提示司机减速

表 2 超载原因

a）驾驶员因素 控制：安全意识淡薄、利益驱动，有超载习惯 b）车辆因素 控制：车辆制动系统制动能力不足 c）道路环境因素 控制：道路条件较差（坡度过大、湿滑等）使车辆制动能力不足 d）检查管理因素 控制：超载检查不到位，不能有效整治超载

表 3 没有按照安全合理路线行驶原因

逆向行驶 a）驾驶员因素 控制：疲劳驾驶、酒驾、毒驾导致注意力不集中，驶入错误车道 b）车辆因素 控制：车辆方向控制系统失效 c）道路环境因素 控制：道路条件较差（施工等）迫使司机驶入错误车道 d）检查管理因素 控制：车道划分不明显、隔离设施不到位；疲劳驾驶、酒毒驾检查不到位	不安全超车 a）驾驶员因素 控制：超车时机判断错误 b）车辆因素 控制：超车时制动、动力、方向控制系统不足以支持安全超车 c）道路环境因素 控制：道路条件（陡坡急弯、路面狭窄等）不支持超车 d）检查管理因素 反馈：相关警示标志设置不到位	车辆冲出道路 a）驾驶员因素 控制：疲劳驾驶、酒驾、毒驾等导致的注意力不集中 反馈：不能有效判断道路路线 b）车辆因素 控制：车辆制动、方向控制系统失效 c）道路环境因素 控制：道路条件不佳（陡坡急弯） d）检查管理因素 控制：防护措施设置不足 反馈：相关警示标志设置不到位

3.2 STPA 分析结果

通过 STPA 方法，从驾驶员因素、车辆因素、道路环境因素、检查管理因素等方面系统识别了引起道路交通事故的技术、社会因素，关注安全控制与反馈的有效性，比较清晰地展现了各因素间的交互关系，不仅发现了人为失误，也进一步发现了导致人为失误的客观因素，对从源头上降低交通事故发生率有重要意义。

4 讨论与结论

4.1 STPA 方法优点

通过理论分析与应用分析发现，STPA 方法具有以下方面的优点：

第一，STPA 方法最大的优点是将风险识别过程系统化[18]-[20]。通过结构化的分析流程设计和对系统结构的分层，保证分析过程的程序化和科学化。同时系统化的分析视角兼顾各组件的交互式影响带来的风险，使得风险识别不再是单纯的线性分析。

第二，STPA 方法可以更准确的描述某些危险致因[21]-[23]。如在超速分析过程中，传统分析方法一般不区分控制或反馈的过早、过晚和没有，而 STPA 方法对此进行了区分；另外，STPA 方法还对系统结构进行分层，使相关使用者可以更准确、更有针对性地分析相关原因。

第三，STPA 方法可以进行模块化分析，提高分析效率[24]-[26]。一旦系统危险发生改变或者需要分析其它风险时，传统的风险识别方法需要从头重新开始分析，耗费人力、财力、物力，而 STPA 方法采用分层控制结构，系统危险发生改变或分析其它风险时只需分析新的结构和新产生的交互影响，在一定程度上提高了风险识别的工作效率。

第四，STPA 方法对高新技术系统的分析更有效[27]。STPA 方法产生于航空航天领域，其设计目的就是解决高新技术条件下复杂系统的安全性问题。STPA 方法在系统设计阶段的风险识别效率较高，可为高新技术系统的研发提供支撑。同时，STPA 方法不仅可以识别硬件问题也可以识别软件问题，为对软硬件要求都较高的高新技术系统风险分析提供了新手段。

4.2 STPA 方法缺点

目前，STPA 方法也存在以下不足需要进一步改进：

第一，对分析对象相关领域的知识要求更高，一般需要多部门的协作。STPA 方法是一种系统分析方法，要求分析人员对系统的各组件工作模式、模块间的交互作用有较深了解，单一领域的技术分析人员不可能有效使用 STPA 方法。

第二，没有界定系统分层控制划分标准，导致分析不足或过量。STPA 方法的关键步骤是划分分层控制结构，但并没有相应原则或标

准确定分析的最低层级，可能会导致分析的不足或过量，导致风险识别不到位或资源的浪费。

4.3 主要结论

本文以 STAMP 模型的内在逻辑为主线，深入分析了 STAMP 模型的主要理论内容及其主要实现技术 STPA 方法，并以交通事故原因分析为例检验了模型和方法的有效性，较以往模型研究更全面、方法分析更具体。STAMP 模型为风险识别提供了新的视角和系统化的分析思路，以 STAMP 为基础产生的 STPA 方法是相关思想在风险识别中的具体化。STPA 方法在一些方面比传统风险识别方法有较大优势，其在高新技术复杂系统等非传统风险识别领域的应用前景将十分广阔。

5 参考文献

[1] 甘传付，曹宏炳，黄允华等. 基于 FMECA 、FTA 的故障诊断和故障预报. 系统工程与电子技术，2002,24（11）：127-130.

[2] 张建国,黄文敏.大型机械产品 FMEA 和 FTA 综合分析方法. 机械设计与制造，2000（1）：1-3.

[3] 郑贤斌，陈国明. 基于 FTA 油气长输管道失效的模糊综合评价方法研究. 系统工程理论与实践，2002,2:139-144.

[4] Vinnem J. E. Hestad, J. A. Kvaløy J. T. Skogdalen J. E. Analysis of root causes of major hazard precursors (hydrocarbon leaks) in the Norwegian offshore petroleum industry. Reliability Engineering & System Safety, 2010, 1142-1153.

[5] Kishawy H. A. Gabbar H. A.. Review of pipeline integrity management practices. International Journal of Pressure Vessels and Piping, 2010,373-380.

[6] 秦彦磊，陆愈实，王娟. 系统安全分析方法的比较研究. 中国安全生产科学技术，2006，2(3): 64-67.

[7] Leveson N. G. Engineering a safer world: Systems thinking applied to safety. MIT Press, 2011.

[8] Leveson N. G. A new accident model for engineering safer systems. Safety Science 2004,42(4): 237-270.

[9] Nelson P. S. A STAMP Analysis of the Lex Comair 5191 Accident . Sweden: Lund University，2008.

[10] Song Y. Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis. City of Hamilton: Mcmaster University,2012.

[11] Altabbakh H. AlKazimi M. A. Murray S. et al. STAMP e Holistic system safety approach or just another risk model? Journal of Loss Prevention in the Process Industries, 2014(32),109-119.

[12] 阳小华，刘杰，刘朝晖等. STAMP 模型及在核电站 DCS 安全的应用展望. 核安全，2013，12（3）: 42-47，88.

[13] 李娟，汪厚祥，林海涛. 基于 STAMP 的舰载作战系统软件安全研究. 舰船科学技术，2010,32（9）：63-66,75.

[14] 刘金涛.基于 STPA 的需求阶段的高速列车运行控制系统安全分析方法研究. 北京：北京交通大学，2015.

[15] Leveson N. Couturier M. Thmoas J. et al. Applying system engineering to pharmaceutical safety. Journal of Healthcare Engineering, 2012,(3):391-414.

[16] Kazaras K. Kirytopoulos K. Rentizelas A. Introducing the STAMP method in road tunnel safety assessment. Safety Science, 2012, 50(9):1806-1817.

[17] David M. James B. W., Risk Assessment for a Chemical Spill into a River. Journal of Risk Analysis and Crisis Response, 2013(3): 116- 126.

[18] 何杰，张娣，张小辉等. 基于 FTA-——Petri 网的地铁火灾事故安全性研究. 中国安全科学学报，2009,19（10）：77-82.

[19] 马从国，赵德安，王建国. 基于故障树分析的增氧机控制系统可靠性动态风险评价. 中国农机化学报，2016，37（4）：211-216.

[20] 李小勋，张超. 基于的形式化安全性分析

计算机应用与软件，2012,29(7):282-285.

[21] Trotter M. J., Salmon P. M., Lenne M. G. Impromaps: Applying Rasmussen's Risk Management Framework to improvisation incidents. Safety Science, 2014, 64(0): 60-70.

[22] 仲景冰，李惠强，吴静. 工程失败的路径及风险源因素的 FTA 分析方法. 华中科技大学学报（城市科学版），2003,20（1）：14-17.

[23] 徐磊，王丹，宋德刚等. 基于 FTA 和贝叶斯网络的动车组制动系统故障分析. 制造业自动化，2016,38（2）：51-55.

[24] 汪进. 核电厂概率安全评价中先进故障树分析方法研究. 合肥：中国科学技术大学，2014.

[25] 马皖，王莹，陈林等. 基于复杂网络分析的软件高危缺陷评估方法. 计算机科学与探索，2014（8）：956-965.

[26] 杨静. 软件项目风险识别及评价模型研究. 南京：东南大学，2006.

[27] 姬忠孝，江国华. 一种基于 FTA 和 FDG 的安全关键函数定位方法. 计算机与现代化，2016（4）：85-89,122.