中文引用格式:吴海涛,黎双喜.高铁应急调度STAMP/STPA安全性分析[J].中国安全科学学报,2021,31(6):113-120.
英文引用格式:WU Haitao, LI Shuangxi.High-speed railway emergency dispatching safety analysis based on STAMP/STPA[J].China Safety Science Journal, 2021,31(6):113-120.

高铁应急调度STAMP/STPA安全性分析*

吴海涛[1,2,3]副教授,黎双喜[1]
(1 西南交通大学 交通运输与物流学院,四川 成都 611756;
2 综合交通运输智能化国家地方联合工程实验室,四川 成都 611756;
3 综合交通大数据应用技术国家工程实验室,四川 成都 611756)

中图分类号:X913 文献标志码:A DOI:10.16265/j.cnki.issn1003-3033.2021.06.015
基金项目:国家自然科学基金资助(51605398);四川省科技厅软科学项目(2020JDR0142);成都市科技局软科学项目(2020-RK00-00080-ZF)。

【摘 要】 为克服传统安全分析模型不能评估高铁调度系统中组件之间复杂交互的缺陷,基于系统理论的事故过程模型(STAMP),将高铁应急指挥系统中人员与设备之间交互安全性问题视作系统控制和反馈问题,构建高铁应急调度控制反馈模型,识别系统安全风险与约束;采用系统理论过程分析法(STPA),分析不安全控制行为及诱发不安全控制行为的控制缺陷;基于台高铁脱轨事故实例分析,验证STAMP/STPA应用于高铁应急调度安全分析的有效性。结果表明:构建的高铁应急调度控制反馈模型可分析得到高铁应急调度指挥的风险因素为感知或执行误差、决策失误、接收或执行时延;同时通过该模型可演绎安全约束失效路径。

【关键词】 高铁应急调度; 系统理论事故过程模型(STAMP); 系统理论过程分析法(STPA); 交互; 安全约束; 控制缺陷

High-speed railway emergency dispatching safety analysis based on STAMP/STPA

WU Haitao[1,2,3], LI Shuangxi[1]
(1 School of Transportation and Logistics, Southwest Jiaotong University, Chengdu Sichuan 611756, China;
2 National United Engineering Laboratory of Integrated and Intelligent Transportation, Chengdu Sichuan 611756, China; 3 National Engineering Laboratory of Comprehensive Transportation Big Data Application Technology, Chengdu Sichuan 611756, China)

Abstract: In order to overcome defect that traditional safety analysis models cannot evaluate complex interactions between components in the high-speed railway dispatching system, based on system theory, STAMP treats interaction safety between personnel and equipment in high-speed railway emergency command system as a system control and feedback problem, high-speed railway emergency dispatch control feedback model was constructed, and system safety risks and constrain were identified. STPA was used to analyze unsafe control behavior and control defects inducing unsafe control behavior. Validity of STAMP/STPA applied to safety analysis of high-speed railway emergency dispatch was verified based on case

* 文章编号:1003-3033(2021)06-0113-08; 收稿日期:2021-03-05; 修稿日期:2021-05-08

analysis of high-speed railway derailment accident in Taiwan. The results show that risk factors of emergency dispatch command of high-speed railway can be analyzed by feedback model of emergency dispatch control perception or execution error, decision-making error, receiving or execution delay. At the same time, failure path of safety constraint can be deduced by model.

Keywords: high-speed railway emergency dispatching; system-theoretic accident model and process (STAMP); system-theoretical process analysis (STPA); interaction; safety constraint; control defects

0 引 言

高铁长期担负着繁重的人员运输任务，一旦出现指挥-响应失误，致使列车速度或位置异常，将严重威胁人员、设备和环境安全。2008 年胶济铁路重大事故[1]，由于人为因素，造成 72 人死亡、416 人受伤。而且，应急调度系统内部人-人，人-设备交互繁多，外部环境多变，影响列车失控的风险因素增多且关联性增强。因此，防止应急指挥-响应失误并控制其灾变事故是保障高铁安全运行的重中之重。

诸多学者对此开展了研究，李凯等[2]基于故障树，分析高铁列车调度子系统的可靠性，得出故障出现的因果关系；张艳潮[3]采用预先危险性分析法，识别出高速铁路运营安全影响因素；秦伟杰[4]采用风险链评估方法，以风险事件概率和事故后果严重程度等指标，评估高铁行车调度系统的安全性。然而，此类基于故障类型的事故模型只能解决故障事件对安全性影响的线性关系，忽略了系统各组成成分之间的耦合性，未能分析由于系统要素间交互不当而导致的事故[5]。2004 年，国外学者 LEVESON[6]提出了一种新的基于系统理论事故过程模型（System-Theoretic Accident Model and Process，STAMP），将系统视为一个层次化控制结构，事故的发生是由于不当控制和不满足安全约束所造成的；LEVESON 等应用 STAMP 模型调查挑战者号航天飞机爆炸事故致因[7]。之后又有相关研究将其应用于医学事故调查[8]、锂离子能开发[9]、网络物理系统[10]等领域。国内学者赵江平等[11]将 STAMP 模型运用于危化品道路运输事故分析；刘炳琪等[12]基于 STAMP 模型分析了飞机差动刹车纠偏过程；孟祥坤等[13]基于 STAMP 分析了深水井控过程中的关键风险因素；李华等[14]利用 STAMP 分析江西一冷却塔倒塌的事故原因并进行定量评估。尽管 STAMP 已在大部分系统工程领域应用，且效果较好，然而针对高铁应急调度系统尚缺乏系统有效的研究手段。

鉴于此，笔者拟应用 STAMP 构建高铁应急调度控制反馈模型，从系统理论角度分析高铁应急指挥安全性，同时，通过实证剖析台自强号高铁脱轨事故，探寻事故发生机制及动态变化过程，以期提高应急调度安全水平。

1 STAMP/STPA 机制

1.1 STAMP 基本原理

复杂系统的安全性可表示为，某一具体环境下由系统相关元素相互作用而产生的一种涌现特性[15]，当系统组件、人员、环境以及社会管理因素间产生复杂交互作用而控制失误时即导致事故[16]。系统安全评估需要识别系统内潜在不安全因素，同时立即实施控制约束手段。

由于复杂系统子系统间、系统与环境间包含了信息、物质及能量的相互作用[17]，欲分析其安全性就要分清系统中存在的功能组件以及对应的逻辑控制关系，剖析各功能组件是否会接收到外部环境干扰，然后定义系统正常运行的控制要求。根据系统逻辑控制结构，STAMP 主要依据事件发生的时间与顺序，识别复杂动态控制过程的安全威胁来进行安全分析。STAMP 方法提供了 3 种基本的控制缺陷来分析复杂系统安全性[19]，具体包括：控制指令不足或错误（即不安全控制行为）；不充分执行控制行为；反馈信息不足或错误。

1.2 STPA 分析方法

系统理论过程分析法（System-Theoretic Process Analysis，STPA）是一种基于 STAMP 的系统安全评价方法，通过建立由执行器、控制器、控制过程以及传感器组成的控制反馈回路（图 1）[20]，分析控制行为在时间、性能及逻辑上的非正常状况，识别不安全的控制行为。STPA 的实施由 4 个步骤组成[21]：识别引发事故的系统条件或状态，界定系统风险；建立安全控制结构，辨识系统各组成部分之间的关系，分析安全要求和限制条件；辨识不安全控制行为引起

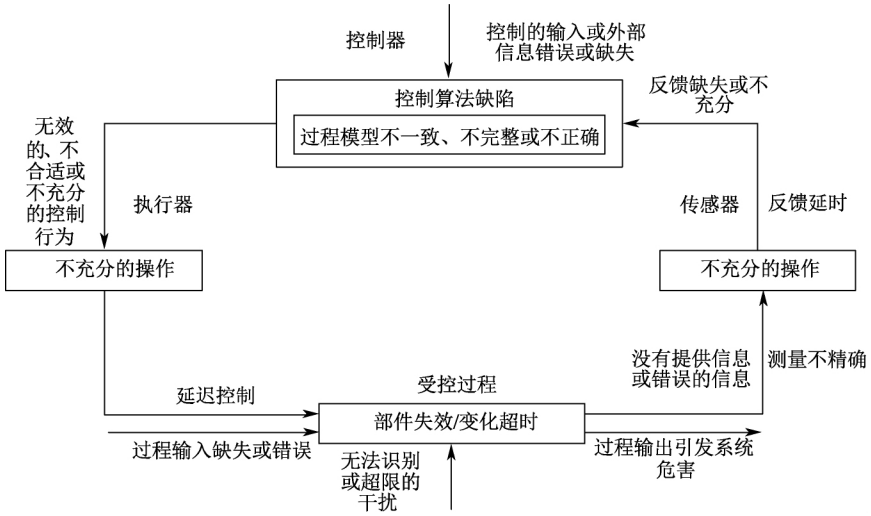

图 1　STAMP 安全控制回路

Fig.1　Safety control loop based on STAMP

的约束失效，STPA 涵盖了不安全控制行为的 4 种类型，即无控制行为、错误或不安全的控制行为、延迟作用的控制行为、过早结束的控制行为；分析不安全控制行为产生的关键致因。

2　高铁应急调度指挥 STAMP 分析

STAMP/STPA 方法与其他安全分析方法的相似之处在于它们均以辨识系统存在的风险为首要目标。不同的是，传统的安全分析方法通过分析获得系统各组成部分的风险概率；而 STPA 方法可以识别出调度指挥响应过程中人-人、人-机交互间控制指令的不足或错误、控制行为的不充分执行与控制信息反馈的不足或错误等状态，根据调度指挥系统控制反馈信息通道中的不安全状态，分析应急调度的安全性。

2.1　高铁应急调度指挥系统安全风险与约束

高铁列车通常实行自动化运行，当发生应急状况时，调度员需协调多个工种来保证列车维持安全距离、安全速度及遵守运行计划，其工作量及心理压力瞬时上升，可能遗漏或提供错误控制指令、错误理解反馈信息等，致应急过程失控使列车超出安全距离、安全速度及违反运行计划，以至引发事故。

因此，将“列车在应急过程中超出安全距离、超出安全速度、违反运行计划”作为系统级风险，将“应急过程中调度员应采取措施避免列车超出安全距离、安全速度、违反运行计划”作为与该风险相关的系统级安全约束。

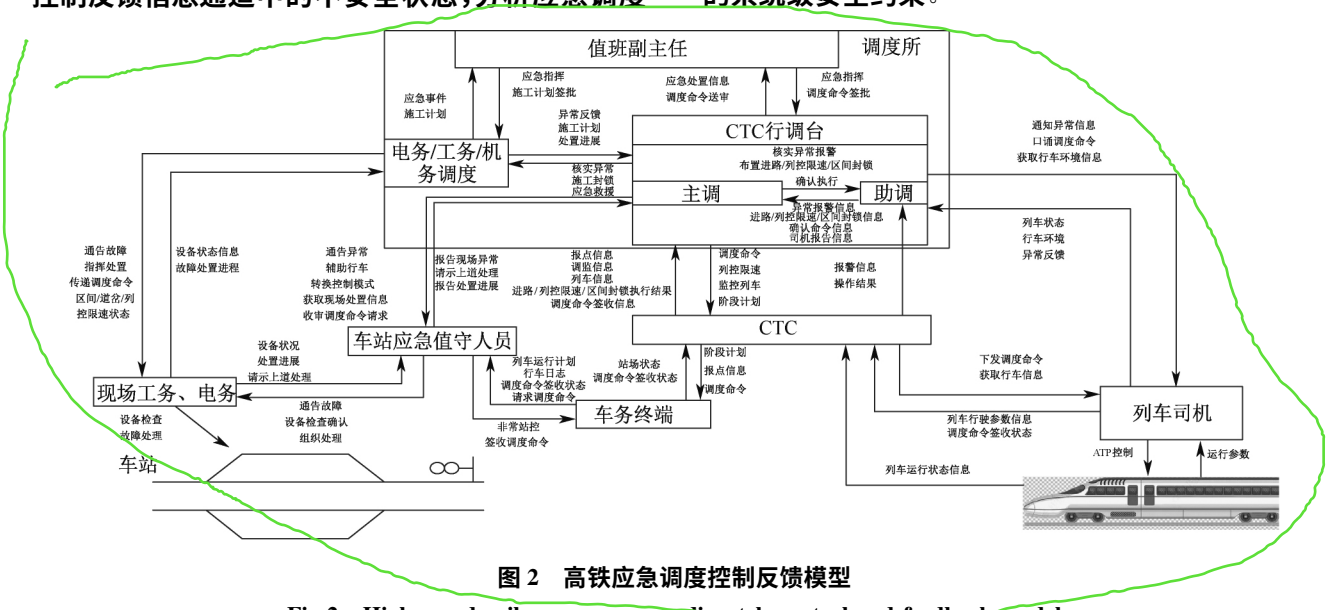

图 2　高铁应急调度控制反馈模型

Fig.2　High-speed railway emergency dispatch control and feedback model

2.2 定义安全控制结构

为保证应急调度指挥的安全性，最合理可行的方法是在调度指挥过程中严格控制主调与助调的规则化操作，并在应急处理初期及时约束。根据图1中安全控制回路、结合调度集中系统(Centralized Traffic Control，CTC)功能结构、人员及设备(如列车自动保护系统(Automatic Train Protection，ATP))交互的信息流，建立高铁应急调度控制反馈模型(图2)。图2中主调代表列车调度员，助调代表助理调度员。

图2展示了各人员及设备间的控制反馈关系，在确定行车中发生异常状况后，调度员根据反馈的事件信息发出控制指令，各指挥-响应人员形成上下层控制关系，并结合各反馈信息判断是否行车，以防止列车超出速度、距离限制，违反调整计划，有效完成整个应急过程。应急指挥过程中主调、助调及司机之间的控制行为分别见表1—表3。

表1 应急指挥过程主调控制行为

Tab.1 Train dispatcher's control behavior during emergency command process

业务员	主调
值班副主任	①通知异常；②调度命令送审
助调	①布置或取消进路/列控限速/区间封锁；②确认操作执行；③核实异常有无及类型
工务/电务/机务调度	①核实异常；②施工封锁；③应急救援；④获取现场行车状态及处置信息；⑤审批施工计划申请
司机	①通知异常信息；②口诵调度命令
车站应急值守人员	①通知异常并组织人员上道；②通知辅助行车/转换CTC控制模式；③获取现场处置信息；④接收并审核调度命令申请

表2 应急指挥过程助调控制行为

Tab.2 Assistant dispatcher's control behavior during emergency command process

业务员	助调
值班副主任	①通知异常
主调	①反馈进路/列控限速/区间封锁布置或取消信息；②确认操作命令信息；③反馈助调终端报警信息；④反馈司机报告；⑤核实异常有无及类型
工务/电务/机务调度	①获取现场行车状态处置信息
司机	①通知/获取异常信息；②获取列车状态/行车环境信息
车站应急值守人员	①通知异常信息并组织人员上道；②获取现场处置信息

表3 应急指挥过程司机控制行为

Tab.3 Train driver's control behavior during emergency command process

业务员	主调	助调
司机	①反馈列车运行状态/行车环境/异常信息；②签认调度命令	①反馈列车运行状态/行车环境/异常信息

2.3 不安全控制行为分析

按照STAMP/STPA方法，根据4种不安全控制行为分类，辨识应急指挥过程中存在的不安全控制行为，通过对不安全控制行为施加安全约束来减少、消除其对应急流程设计、操作等多个环节造成的不利影响。以行车调度员、司机及CTC设备为例，应急指挥-响应过程中，识别出的不安全控制行为分别见表4和表5。

表4 行车调度员的不安全控制行为

Tab.4 Traffic dispatchers' unsafe control behavior

业务员	无任何控制行为	错误或不安全的控制行为	延迟作用的控制行为	过早结束的控制行为
行车调度员	①未监测异常； ②未核实异常； ③未调整列车运行计划； ④未通知司机采取措施； ⑤未通知值班副主任盯控； ⑥未布置或取消进路/列控限速/区间封锁； ⑦未通知车站应急值守人员组织上道处理	①未执行“2人确认”核实异常/发布命令即操作CTC； ②列车运行计划调整错误/无效； ③未得到工务/电务/机务/司机/车站应急值守人员反馈即组织行车； ④错误布置或取消进路/列控限速/区间封锁； ⑤仅口头通知司机调度命令后未书面下发	①调度员监测到异常过晚； ②调度员通知值班副主任/车站应急值守人员/电务/工务/机务/司机过晚致事态扩大； ③布置进路/列控限速/区间封锁过晚； ④过晚调整列车运行计划	①未有效监测异常即结束监测行为； ②列控限速/区间封锁有效时间过短

表 5　司机不安全控制行为

Tab.5　Driver´s unsafe control behavior

业务员	无任何控制行为	错误或不安全的控制行为	延迟作用的控制行为	过早结束的控制行为
司机	①行车过程未监测异常; ②未报告行车调度异常/行车环境信息; ③发现异常后未控制列车	①错误操作 AYP/列车; ②行车环境/异常信息反馈内容/对象错误	①行车环境/异常信息监测及报告过晚; ②ATP/列车操作过晚	①未有效监测异常即结束监测行为; ②ATP/列车操作不彻底

2.4　诱发不安全控制行为的控制缺陷分析

根据辨识的不安全控制行为,分析不安全控制行为的控制缺陷,大致可分为以下 8 种:

1) 调度员心理状态不佳。主要有: 注意状态不良(如对任务关注过多/过少) 、由任务复杂度及时间压力引起的紧张/焦虑感、性格特征(责任感不足、寻求风险等) 。

2) 调度员生理状态不佳。如调度员可能处于疲劳状态、任务超出调度员身体承受阈值等。

3) 调度员训练不足缺乏经验。主要包括对进路布置、临时限速、施工封锁、调整运行计划的设置规范不熟。

4) 操作手册文本描述不恰当或缺失。这是指可供调度员使用的应急预案文本的缺陷。

5) 不适宜的环境、组织及团队因素。

6) CTC 及 ATP 内部信息模块未连线/控制算法逻辑错误致未产生或产生错误反馈信息。

7) CTC 网络通信设备(调度通信系统、G 网电话及无线闭塞中心等) 信号中断或不稳定致控制人员未获取充分信息。

8) 其他影响因素。如外部(集团公司) 指挥信息不正确; 外界信号干扰; CTC 显示器和控制器布置不合理; 车载及地面设备机械故障; 通信电缆质量不达标; 电力系统供电中断等。

综上所述,应急调度指挥系统的风险因素可分为 3 类: 感知/执行误差、决策失误、接收/执行时延。

3　台自强号高铁脱轨事故案例分析

2018 年 10 月 21 日,台铁第 6432 次自强号列车超速脱轨,事故造成旅客 18 人死亡,267 人受伤。司机行车中发现异常未及时停车报告、擅自隔离 ATP,调度在列车动力异常时依然制定滑行策略,期间与司机多次通信未能排除异常,最终滑行过程列车超速造成事故。

与该次事故有关的控制器包括: 司机、行车调度、机车调度、机务段检查员、ATP 系统及 ATP 远端监视器。与事故相关控制器失效原因分析如下:

司机应在行车中根据 ATP 显示信息控车且观察列车运行环境,发现异常即报告行车调度。然而,在该事故中,司机发现列车动力异常后未亲自报告行车调度,控车的同时与机车调度持续沟通,之后擅自隔离 ATP,列车 ATP 远端监视器也未连线,影响了行车调度的决策。司机以错误作业程序行车,低估设备维修的困难程度,制订边行车边检查设备的错误决策,且私自关闭 ATP 致其不能显示列车实时速度,是诱发事故的直观原因。

行车调度负责列车运行的全局把控,需时刻了解列车区间运行状态并作出正确指挥决策,且在调度过程中应以安全为重。该事故中行车调度未能在多个信息源间维持良好通信,知道列车动力异常后未时刻与司机及机车维修员联络,尤其是在列车动力异常时放任列车滑行而非扣停。由此可见其业务及风险感知能力的缺失,是错误指挥的重要原因。

机车调度员应反馈机车设备状况及维修状态至行车调度,该事故中,机车调度接收司机反馈设备状况后,由于其业务能力不足无法给出有效维修措施,并在与司机联络过程中未及时反馈行车调度,在一定程度影响了行车调度员的决策。

机务段检查员本应及时制定正确的列车维修措施,该事故中,其未能给出有效措施恢复列车正常运行,且将维修任务推给其余机车检修人员,可见其业务能力不足。ATP 负责列车速度控制,实时显示列车所处位置实际速度及最高允许速度,该事故中司机误关 ATP 致其未发挥作用,极大影响了司机控车过程。ATP 远端控制器负责将机车室的 ATP 等设备工作状态反馈至行车调度,而在该事故中 ATP 远端控制器未连线致其无法发挥作用,在一定程度上影响了行车调度的决策过程。

对于应急调度指挥系统而言,要想在事故发生前控制多数风险,最好的办法就是制定科学完备的应急指挥流程。该事故的正常应急调度指挥过程的有效控制结构和事故发生时的无效控制结构如图 3 所示(虚线表示脱轨事故中的控制失效环节) 。

调度指挥过程中的不安全控制行为是控制过程

失效的重要诱因。在该次事故中，应急调度指挥过程中存在的不安全控制行为见表 6，控制组件失效原因总结分析见表 7。

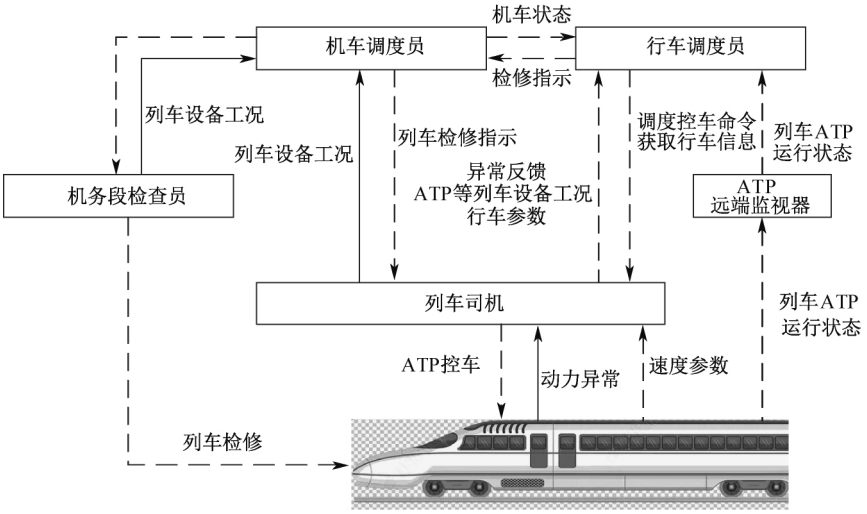

图 3　台自强号高铁脱轨事故中控制结构模型

Fig.3　Control structure model of Taiwan´s Ziqiang high-speed railway derailment accident

表 6　台自强号高铁脱轨事故中不安全控制行为分析

Tab.6　Analysis of unsafe control behavior in derailment of Taiwan´s Ziqiang high-speed railway

控制行为	描述	失效原因
列车速度参数	列车 ATP 发向司机	未发送
ATP 控车措施	司机通过 ATP 控制列车	未实施
列车检修操作	机务段检查员检修列车	错误操作
列车检修建议	机车调度员发向机务段检查员	错误建议
列车检修建议	机车调度员发向司机	错误建议
机车状态	机车调度员发向行车调度员	未发送
检修指示	行车调度员发向机车调度员	未发送
列车行车及设备状况	司机发向行车调度员	未发送
调度控车命令	行车调度发向司机	错误命令
列车 ATP 设备工作状态	列车发向 ATP 远端监视器	未发送
列车 ATP 设备工作状态	ATP 远端监视器发向行车调度	未发送

表 7　台自强号高铁脱轨事故中控制组件失效原因分析

Tab.7　Analysis on causes of failure of control components in derailment of Taiwan´s Ziqiang high-speed railway

控制组件	失效原因
司机	轻视列车动力问题，未报告，未停车，擅自隔离 ATP，错判滑行速度
行车调度	业务能力不足，轻视列车动力问题，错误指示列车滑行，未给出正确行车措施
机车调度	业务能力不足，检修措施错误
机务段检查员	业务能力不足，检修措施错误
ATP 系统	司机擅自关闭，致未正常工作
ATP 远端监视器	未联机工作

3.1　安全约束建议

由不安全控制行为生成相应的安全约束，以具体的约束条件指导台自强号脱轨事故应急调度过程，同时辨识事故中司机、地面或车载设备及行车调度间的安全约束缺失，进而改进图 2 中高铁应急调度控制反馈模型，指导调度流程安全性设计。在图 2 模型中，需要施加安全约束的具体位置为：行车调度与司机及 CTC、CTC 与司机、司机与列车控制反馈回路。以下为详细的安全约束建议：

1）确保 ATP 远端监视系统正常运行。由图 3

中事故控制结构模型可知，列车机载 ATP 远端监视器未联机工作。台铁中所有类型机车均安装有 ATP 远端监视器，而唯独普悠玛型号列车仅安装而未投入使用，甚至司机也不知列车已安装该装置。行车调度对列车状态的感知能力仅依赖于调监屏列车位置显示及与司机的口头沟通。列车状态感知途径单一以及基于人工逻辑的危险判断方式都会影响行车安全。因此，保证 ATP 远端监视器正常工作，是提高指挥系统冗余度保证行车安全的有效途径。

由于国内采用中国列车运行控制系统，与列控设备动态监视系统留有接口，其负责实时监控 ATP 的工作状态，并将 ATP 故障信息、机车电源信息及司机动作信息传输至地面，因此，无需对国内应急调度指挥系统补充此条约束内容。

2) 通过培训提高相关人员业务能力及危险感知能力。该事故中司机在列车动力异常时擅自隔离 ATP，未报告行车调度，维修过程通话检修的同时控制行车；行车调度未及时获取列车运行信息且制定错误滑行决策；机车调度及机车维修人员采取无效措施修复机车动力且未将具体状况通告行车调度。由此可见相关人员业务能力及危险感知能力严重不足。相应的安全约束建议为：增加有效的培训过程，提高调度及司机业务能力及危险感知能力。

对应图 2 模型，针对行车调度与司机、工务、电务、机务、车站应急值守人员的控制反馈回路，仍需加强平时业务能力培训，总结各历史事故经验，做到有备无患。

3) 制定详细有效的应急行车预案以减少人员失误。该事故中列车在动力异常情况下依然行驶，司机与行车调度沟通缺乏且严重违反 ATP 隔离规定，在动力异常时仍未减速；行车调度未考虑列车实际运行参数主观制定滑行策略；机车调度及维修人员无法提出有效措施，也未报告行车调度；种种迹象表明：台高铁行车缺乏一套有效的应急处理程序，因此，相应的安全约束建议为：制定可靠的应急行车预案，尽量减少处置过程中人员主观判断。为增加图 2 模型可靠性，此条安全约束建议同样适用于国内高铁应急行车处置。

4) 加派助理调度员负责司机及列车状态收集，确保调度对行车信息的全局把控。该事故中，行车调度与司机通信时未详细掌握司机已实施操作、ATP 及动力设备具体状况，亦未主动询问相关控车信息。相应的安全约束建议为：加派专门的助理调度员，在应急指挥过程向行车调度给出完备的列车信息，减少行车调度主观判断异常状况的风险性。对应于图 2 模型，针对行车调度与司机控制反馈回路，亦有必要采用该条约束建议。

该次事故的发生涉及人员、设备及组织管理制度等多层面因素，尽管国内和台湾在高铁运行方面存在些许差异，但在总体行车方案上两者思路基本一致，对台高铁事故的分析过程及结果仍对国内高铁行车具有十分强烈的借鉴指导意义。

4　结　论

1) 构建了高铁应急调度控制反馈模型，运用该模型分析调度控制指令传递过程，发现应急调度指挥的风险因素为感知或执行误差、决策失误、接收或执行时延。

2) 基于高铁应急调度控制反馈模型，发现系统各层级及组件之间缺乏足够的控制及反馈，这些因素将导致系统级安全约束逐步失效，进而导致事故发生。

参 考 文 献

[1] 佚名. 胶济铁路列车相撞特大事故 [J]. 瞭望，2008(18)：29.

[2] 李凯，王明起，汪颖，等. 基于故障树分析的高速铁路列车调度子系统可靠性的探讨 [J]. 交通与运输：学术版，2013(1)：136-138.
LI Kai，WANG Mingqi，WANG Ying，et al. The discussion about the stability of the high-speed railway train scheduling subsystem in fault tree analysis [J]. Traffic & Transportation，2013(1)：136-138.

[3] 张艳潮. 高速铁路运营安全风险分析与评估 [D]. 大连：大连交通大学，2017.
ZHANG Yanchao. High-speed railway safety risk analysis and assessment [D]. Dalian：Dalian Jiaotong University，2017.

[4] 秦伟杰. 高速铁路行车调度系统安全风险分析 [D]. 成都：西南交通大学，2016.
QIN Weijie. Analysis of safety risk in high-speed railway dispatching system [D]. Chengdu：Southwest Jiaotong University，2016.

[5] HANEET S M，THOMAS B，SUDEEP P. Application of systems theoretic process analysis to a lane keeping assist system [J]. Elsevier Limited，2017，167(11)：177-183.

[6] LEVESON N. A new accident model for engineering safer system [J]. Safety Science, 2004, 42(4): 237-270.
[7] LEVESON N G. Technical and managerial factors in the nasa challenger and columbia losses: looking forward to the future [M]. New York City: Mary Ann Liebert Press, 2008: 1-15.
[8] LEVESON N, SAMOST A, DEKKER S, et al. A systems approach to analyzing and preventing hospital adverse events [J]. Journal of Patient Safety, 2020, 16(2): 1-7.
[9] DAVID R, ADAM W. Analyzing system safety in lithium-ion grid energy storage [J]. Journal of Power Sources, 2015, 300(30): 460-471.
[10] IVO F, KIERAN M, PAUL S, et al. STPA-safesec: safety and security analysis for cyber-physical systems [J]. Elsevier Limited, 2017, 34(2): 183-196.
[11] 赵江平，刘小龙，东淑，等. STAMP 模型在危化品道路运输事故分析中的应用研究 [J]. 中国安全生产科学技术，2020，16(5)：160-165.
ZHAO Jiangping, LIU Xiaolong, DONG Shu, et al. Study on application of STAMP model in analysis on road transportation accidents of hazardous chemicals [J]. Journal of Safety Science and Technology, 2020, 16(5): 160-165.
[12] 刘炳琪，胡剑波，刘畅，等. 飞机差动刹车纠偏过程的 STAMP/STPA 安全性分析 [J]. 哈尔滨工业大学学报，2020，52(4)：55-58.
LIU Bingqi, HU Jianbo, LIU Chang, et al. STAMP/STPA safety analysis of aircraft differential braking correction process [J]. Journal of Harbin Institute of Technology, 2020, 52(4): 55-58.
[13] 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(2)：131-139.
MENG Xiangkun, CHEN Guoming, ZHANG Xiaojin, et al. Safety analysis of deepwater well control based on STAMP/STPA [J]. Journal of China University of Petroleum: Edition of Natural Science, 2019, 43(2): 131-139.
[14] 李华，金萌，钟兴润. 基于 STAMP 模型的建筑事故致因因素定量分析方法研究 [J]. 中国安全生产科学技术，2020，16(4)：169-175.
LI Hua, JIN Meng, ZHONG Xingrun. Research on the quantitative analysis method for the cause of construction accidents based on the STAMP model [J]. Journal of Safety Science and Technology, 2020, 16(4): 169-175.
[15] 王瑛，孙赟，李超，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(9)：68-73.
WANG Ying, SUN Yun, LI Chao, et al. Safety analysis of military aircraft flight training based on STAMP model [J]. China Safety Science Journal, 2018, 28(9): 68-73.
[16] OUYANG MIN, LIU Hong, MING Huiyu, 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.
[17] 马刚，杜宇鸽，杨熙，等. 复杂系统风险评估专家系统 [C]. 信息安全漏洞分析与风险评估大会，2014：250-269.
[18] 王起全，吴嘉鑫. 基于 STAMP 模型的地铁拥挤踩踏应急联动系统设计 [J]. 中国安全科学学报，2016，26(12)：158-162.
WANG Qiquan, WU Jiaxin. Designing a linkage system for response to subway stampede accidents based on STAMP model [J]. China Safety Science Journal, 2016, 26(12): 158-162.
[19] 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 Lei, HU Jianbo. Safety analysis of wheel brake system based on STAMP/STPA [J]. Acta Aeronautica et Astronautica Sinica, 2017, 38(1): 241-251.
[20] 李京生，赵林，王阳，等. CRES 的危害因素识别方法: 以 EETD 为例 [J]. 中国安全科学学报，2019，29(1)：106-111.
LI Jingsheng, ZHAO Lin, WANG Yang, et al. Study on method for identifying hazardous factors in CRES: EETD taken as an example [J]. China Safety Science Journal, 2019, 29(1): 106-111.
[21] 马文·拉桑德. 风险评估理论、方法与应用 [M]. 北京：清华大学出版社，2013：127-134.

作者简介： 吴海涛 (1981—)，男，山东烟台人，博士，副教授，主要从事交通运输系统安全性与人因可靠性、交通运输网络可靠性等方面的研究。E-mail: wuhaitao@swjtu.cn。