文章编号：1005-8451（2016）12-0011-04

临时限速服务器模型的建立与HAZOP分析

刘嫦娥
（铁道第三勘察设计院集团有限公司，天津 300251）

摘 要：从不同角度对临时限速服务器进行建模，建立了临时限速服务器的参考结构模型、功能分层模型和状态转移模型；采用危险与可操作性分析（HAZOP）方法分别对3种模型进行风险分析，建立较为全面的危险源数据库，可以作为系统运营期管理的依据。

关键词：临时限速服务器；参考结构模型；功能分层模型；状态转移模型；HAZOP
中图分类号：U231.92：TP39 **文献标识码：**A

Model of temporary speed restriction server and HAZOP analysis

LIU Chang'e
(The Third Railway Survey and Design Institute Group Corporation, Tianjin 300251, China)

Abstract: From different angles, this article established reference architecture model, functional hierarchical model and state transition model of temporary speed restriction server(TSRS), Hazard and operability (HAZOP) analysis method was used to analyze the risk of three models. A more comprehensive hazards source database was established which could be used as the basis of system operation period management.

Key words: temporary speed restriction server(TSRS); reference architecture model; functional hierarchical model; state transition model; hazard and operability (HAZOP)

临时限速的设置、下达和取消均在调度中心进行，调度中心设置列车控制系统专用的临时限速服务器（TSRS ,Temporary Speed Restriction Server）。TSRS 存储临时限速命令并不断检查执行时机，到达执行时间的限速命令被激活后，通过安全数据网下达给无线闭塞中心（RBC，Radio block center）和列车控制中心（TCC,Train Control Center）分别执行处理。

TSRS 对行车安全至关重要，一旦 TSRS 失效，可能导致列车在限速区段超速，引发列车追尾等安全事故。所以，对 TSRS 进行安全风险分析，寻找 TSRS 存在的风险是非常有必要的。

危险与可操作性分析（HAZOP ,Hazard and Operability Study）方法是一种系统全面的危险分析方法，广泛应用于各个行业的危险性分析。HAZOP 法在国外应用广泛，是国外铁路行业的安全与风险评估的主要方法。在国内，国家安监总局已将其作为重点推广的危险分析方法。

风险评估 [1] 直接关系到系统的安全，风险评估越全面，系统安全性越高。从不同角度出发，对 TSRS 建立不同的模型进行风险评估，可以有效地提高风险评估的完整性。因此，本文从硬件结构的角度建立了 TSRS 的参考结构模型，从功能角度建立了 TSRS 的功能分层模型，从状态转移的角度建立了 TSRS 的状态转移模型，并对 3 种模型分别进行了 HAZOP 分析。

收稿日期：2016-04-03
作者简介：刘嫦娥，工程师。

1 HAZOP法简介

HAZOP 法是一种以系统工程为基础的结构化的危险分析方法 [2-4]，通过分析工艺图纸和操作规程中可能产生的危险，找出发生危险的原因，提出相应的改善建议和措施。HAZOP 法应用范围广泛，可以用于产品的前期设计阶段，也可用于现有产品的风险评估；不论是连续性的生产过程还是间断性的生产过程，都可以使用 HAZOP 法进行安全与风险分析。

HAZOP 法有 3 种基本的形式 [5-7]：引导词方式、经验式和检查表式。其中，较为常见的是引导词方式。本文使用的是引导词方式。

HAZOP 法包括以下 3 个基本步骤：

（1）分析前的准备。确定分析对象的目标和范围；确定分析小组成员；收集必要资料，包括基础

数据、工艺流程、操作规程等；整理数据资料，将资料整理成适当的表格形式，并制定详细的分析计划；拟定会议时间。

（2）召开分析会议。将系统合理的分解成若干分析节点，每个节点再分解成若干要素，对每个要素搭配引导词形成偏差，分析每一种偏差产生的原因和导致的后果，并提出切实可行的应对措施。

（3）分析文档整理。整理会议记录形成分析文档，根据分析文档形成分析报告，投入执行并反馈执行结果，必要时重新分析部分节点，形成最终的输出报告文档。

2 TSRS参考结构模型与HAZOP分析

2.1 建立TSRS参考结构模型

使用 HAZOP 法进行风险识别的基础是建立一个准确的临时限速服务器参考结构模型。参考结构模型从宏观上对临时限速服务器的风险识别进行界定，可以直观地看出系统的模块组成和系统边界，了解系统环境以及和其它系统之间的关系。参考临时限速服务器技术规范（2012 年版）[8]，临时限速服务器由主机、维护终端、接口单元组成。临时限速服务器的参考结构模型如图 1 所示。

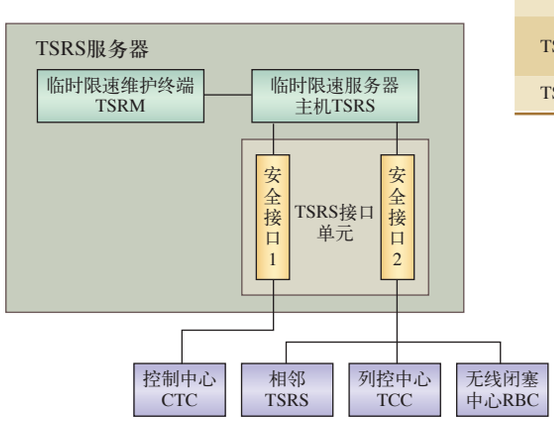

图1 临时限速服务器的参考结构模型

2.2 TSRS参考结构模型的HAZOP分析

以 TSRS 的参考结构模型 [9-10] 的每一个单元模块作为节点进行 HAZOP 分析。这里选择 TSRS 主机为例来说明 HAZOP 分析的过程。此时，分析的节点就是 TSRS 主机，分析的要素是主机板，引导词可以从 No 、As well as、In error、Reverse、More、Part of、Less、Earlier、Later 中选取。引导词和要素相结合即得到危险源。不一定所有的引导词都要用到，要根据引导词和要素的结合情况而定，舍弃无意义、不恰当的引导词。通过筛选，只有 In error 与主机板结合才有意义，即主机板故障，继而分析其发生原因和可能后果，并提出相应的建议措施，如表 1 所示。

表1 TSRS主机单元的危险源数据表

节点	引导词	要素	危险源	发生原因	可能后果	建议措施
TSRS主机单元	In error	主机板	主机板故障	1.过压、过流 2.器件老化 3.主机板可靠性差	TSRS失效	1.设计过压、过流防护电路 2.选用高可靠性的器件 3.定期维护 4.向CTC报警

3 TSRS功能分层模型与HAZOP分析

3.1 建立TSRS功能分层模型

把功能作为分析节点，能够为维修提供很大的便利。当系统出现故障时，可以通过部分功能的失效进行快速定位故障，对照危险源数据库，就能很快找到发生原因和可能后果，从而采取相应的补救措施。以 TSRS 主机单元为例，部分功能如表 2 所示。

表2 TSRS主机的功能分层模型

代码	功能	描述
TSRSH-1	初始化功能	载入本地存储的限速命令信息；对自身的初始化状态进行判定；对TCC的初始化状态进行判定；对RBC的初始化状态进行判定。
TSRSH-2	管理功能	TSRS应具备临时限速命令存储、校验、删除、拆分、设置和取消的管理功能。
TSRSH-3	时钟同步	TSRS应具备保持与CTC系统时钟同步功能。

3.2 TSRS功能分层模型的HAZOP分析

这里选择启动自检功能中的建立通信 [11] 这一要素为例进行分析，分析结果如表 3 所示。

4 TSRS状态转移模型

4.1 建立TSRS状态转移模型

TSRS 的运行过程实际上就是状态转移的过程，研究 TSRS 所有可能所处的状态 [12] 以及不同状态之间相互转移的条件，对安全分析至关重要。对于每一种状态，TSRS 都要完成相应的功能，有些功能有时序要求，如图 2 中用 entry 表示，有些则没有，图 2 中用 do 表示。

将 TSRS 的执行过程分为 6 个状态：停机状态、上电状态、建立通信状态、初始化状态、正常运行

表3　TSRS启动自检功能的危险源数据表

节点	引导词	要素	危险源（偏差）	发生原因	可能后果	建议措施
启动自检功能	No	建立通信	没有建立通信	1.设备完整性检查失败 2.程序逻辑错误	TSRS失效	1.选用高可靠性的硬件模块 2.定期维护 3.规范程序设计 4.加强程序测试、验证与确认
启动自检功能	In error	建立通信	通信建立错误	1.通信协议错误 2.程序逻辑错误	1.信息无法正常收发 2.信息可靠性降低 3.导致列车脱轨 4.影响行车效率	1.规范程序设计 2.加强程序测试、验证与确认 3.提高程序的鲁棒性
启动自检功能	Part of	建立通信	部分通信建立	1.通信接口板故障 2.通信线路破损 3.程序逻辑错误	TSRS失效	1.选用高可靠性的通信接口板 2.选用质量较好的连接线 3.定期维护 4.规范程序设计 5.加强程序测试、验证与确认

状态和系统异常状态。这6个状态之间的转移关系如图2所示。

为了方便HAZOP分析，对每一种状态，我们都做了相应的状态描述，对状态要完成的功能和状态转移的条件进行详细分析和说明，下面对初始化状态的具体描述举例说明，如表4所示。

表4　初始化状态

状态	定义	进入条件	从哪个状态进入
初始化	完成加载本地限速信息，完成自身以及边界和非边界的TCC和RBC限速命令初始化的功能	T6当系统完成通信建立后 T10成功处理初始化异常后	T6 从建立通信完成进入 T10 从系统异常恢复进入
操作		退出条件	退出到哪个状态
1.加载本地限速信息 2.自身限速命令初始化 3.边界TCC及RBC限速命令初始化 4.非边界TCC及RBC限速命令初始化		T8初始化出现异常 T9初始化完成	T8→系统异常 T9→正常运行

4.2　TSRS状态转移模型的HAZOP分析

以TSRS所处的每一种状态作为节点，状态转移条件作为要素进行HAZOP分析，这里以通信建立状态这个节点的T6要素为例，分析结果如表5所示。

表5　通信建立状态的危险源数据表

节点	引导词	要素	危险源（偏差）	发生原因	可能后果	建议措施
通信建立	No	T6	通信建立状态转移至初始化状态失败	程序逻辑错误	TSRS失效	1.选用高可靠性的通信接口板 2.规范程序设计 3.加强程序测试、验证与确认 4.定期维护

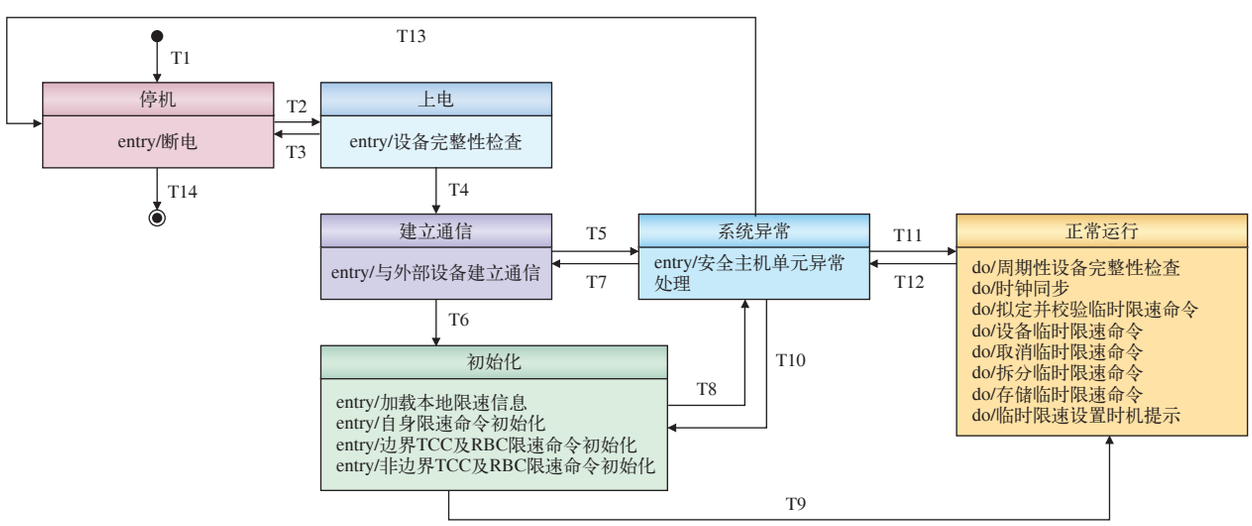

图2　TSRS状态转移模型

5　结束语

参考结构模型从硬件上对TSRS进行建模和HAZOP分析，功能分层模型在此基础上对每一个模块进行详细深入的功能划分和分析，状态转移模型在以上两个模型的基础上分析了TSRS的状态转移过程。由此可见，从参考结构模型到状态转移模型，通过层层深入地对TSRS进行HAZOP分析，得到较为全面的危险源数据库，可以作为TSRS前期设计的参考，可以作为运营期管理的依据，从而有效地降低事故发生率，保障行车安全。

参考文献：

[1] 吴　卫．风险评估技术在铁路信号系统中的应用 [J]．自动化与仪器仪表，2012（2）：122-124.
Wu Wei．Risk assessment techniques used in railway signal system[J]．Automation and Instrumentation，2012(2)：122-124.

[2] Feng Wang, Yankun Zhao, Ou Yang, Jingbo Cai, Mei Deng. Process safety data management program based on HAZOP analysis and its application to an ethylene oxide/ethylene glycol plant[J]. Journal of Loss Prevention in the Process Industries, 2013(26)：6.

[3] Jing Wu, Laibin Zhang, Wei Liang, Jinqiu Hu. A novel failure mode analysis model for gathering system based on Multilevel Flow Modeling and HAZOP[J]. Process Safety and Environmental Protection, 2013(91): 1-2.

[4] S.F. Ávila，F.L.P. Pessoa，J.C.S. Andra-de．Social HAZOP at an Oil Refinery[J]．Proc. Safety Prog，2013(32)：1.

[5] Min An，Yao Chen，Chris J. Baker．A fuzzy reasoning and fuzzy-analytical hierarchy process based approach to the process of railway risk information：A railway risk management system[J]. Information Sciences, 2011, 181(18): 3946-3966.

[6] Nan B.M. Sahar, Syahril Ardi, Suzuki Kazuhiko. HAZOP Analysis Management System with Dynamic Visual Model Aid[J]. American Journal of Applied Sciences, 2010, 7 (7): 943.

[7] Netta Liin Rossing, Morten Lind, Niels Jensen. A functional HAZOP methodology[J]. Computers & Chemical Engineering, 2010 (34).

[8] 中华人民共和国铁道部运输局．临时限速服务器技术规范：铁运 [2012]213 号 [S]. 北京：中华人民共和国铁道部运输局，2012.

[9] 何春明，田振武，史增树．临时限速服务器安全通信协议研究 [J]．铁道通信信号，2011，47（10）：50-52.
He Chunming, Tian Zhenwu, Shi Zengshu．Temporary speed server secure communication protocol study[J]. Railway Signal & Communication，2011，47(10)：50-52.

[10] 贾玉洁．浅谈京广高铁临时限速系统 [J]. 郑铁科技，2013（4）：14-16.
Jia Yujie. TSRS on the Beijing-Guangzhou[J]. Zheng Rail Technology，2013(4): 14-16.

[11] 王　喆，郭艳军．列车控制仿真测试平台中模拟临时限速服务器研究 [J]. 铁路计算机应用，2013，22（3）：13-17.
Wang Zhe, Guo Yanjun．Research on simulate TSRS on train control simulation test platform[J]. Railway Computer Application，2013，22(3)：13-17.

[12] 刘栋青．TSRS 间限速命令状态的判定及迁移设计的研究 [J]. 铁路通信信号工程技术，2013（10）：59-63.
Liu Dongqing．Research on TSRS speed command status determination and migration design [J]. Railway Signal & Communication Engineering，2013（10）：59-63.

责任编辑　徐侃春

（上接 P10）

计划编制的研究 [J]. 铁道学报，2006（4）：17-21.

[6] 张才春，陈建华，花　伟．基于不同检修能力的动车组运用计划研究 [J]. 中国铁道科学，2010（5）：130-133.

[7] 史　峰，周文梁，郁宇卫，等．客运专线动车组运用计划优化模型与算法 [J]. 铁道学报，2011（1）：8-13.

[8] 陈华群．动车组运用计划编制系统相关问题研究 [D]. 成都：西南交通大学，2007.

[9] 张　杰，陈　韬，施福根．客运专线动车组运用计划的计算机编制 [J]. 西南交通大学学报，2006（5）：635-640.

[10] 李　华，韩宝明，张　琦，等．动车组交路计划优化模型与算法研究 [J]. 铁道学报，2013，35（3）：1-8.

[11] 郁宇卫．客运专线动车组运用计划优化研究 [D]. 长沙：中南大学，2009.

[12] 耿敬春．京沪高速铁路动车组运用计划编制相关问题研究 [D]. 成都：西南交通大学，2009.

[13] 陈玲娟．遗传算法在动车组运用计划编制中的应用 [J]. 交通运输工程与信息学报，2009（2）：67-71.

责任编辑　徐侃春