文章编号:1005-0523(2016)03-0068-06

临时限速服务器安全评估研究

张利华,罗志华

(华东交通大学电气与电子工程学院,江西 南昌 330013)

摘要:近年来我国高速铁路飞速发展,越来越多的高速铁路线路投入使用有效的缓解了我国铁路出行的压力。如何保证铁路的安全运行成为了人们亟需研究的问题。临时限速服务器是CTCS-3级列控系统的重要组成部分,其系统安全直接影响到高速铁路的运营安全。文章结合临时限速服务器的实际运行过程,采用安全性分析软件SIMFIA构建临时限速服务器仿真模型,自动生成系统故障树,并计算失效状态最小割集。根据最小割集可以快速找到故障源,从而达到分析临时限速服务器安全性的目的。

关键词:临时限速服务器;安全评估;最小割集;SIMFIA;建模仿真

中图分类号:U284.92 文献标志码:A

DOI:10.16749/j.cnki.jecjtu.2016.03.011

列控系统对于保障铁路运行安全,提高铁路运行效率起到了关键作用,在铁路发展中具有非常重要的地位。临时限速是指除规定的限速,由施工或者维修等原因引起的有计划限速及自然灾害或者设备故障等引起的突发限速。由于临时限速命令主要依据相应的规范,标准来运行操作,依靠经验和直觉制定的规划标准多少会有安全隐患,这些安全隐患可能会演变成系统故障,并最终导致安全事故的发生。为此,许多研究者对列控系统临时限速过程进行了安全分析。文献[1]利用UPPAAL工具对临时限速系统的信息交互过程进行建模仿真,根据系统模型的功能属性,验证了临时限速系统的安全性;文献[2]通过消息顺序图(MSC)对临时限速系统进行建模,这在临时限速系统安全评估中尚属首次,文章通过MSC与时间自动机理论两种方法相结合,根据临时限速系统与外部结构的信息交互过程建立模型,充分验证了系统的活性与安全性;文献[3]使用Rational Rose建模工具中UML建模语言,用UML语言的用例视图和类视图分析和描述了临时限速系统的功能及结构,采用国际公认的V模型,分析了临时限速系统软件的整个生命周期的安全,取得了比较理想的结果。大部分研究者对临时限速系统的研究主要是针对临时限速系统的信息交互过程进行安全评估,但是很多时候,故障往往出自具体的硬件设备模块。

通过使用SIMFIA软件对临时限速系统进行分析,按照其系统的具体功能进行模块化建模仿真,自动生成故障树(FTA),并通过配置模型参数,自动计算每个模块的故障概率。SIMFIA主要根据生成的故障树进行定性、定量分析。故障树(FTA)是对可能造成产品故障的软件、硬件、环境和人为因素进行定性和定量分析,帮助判明可能发生的故障模式和原因,发现系统的薄弱环节并进行相应的改进。通过SIMFIA建立的系统,如果仿真模块发生变化,只要重新生成故障树及其他的数据即可。由于基于模型驱动的SIMFIA软件这种独特的性能和高度自动化的分析优势, 使得安全评估人员可以将更多的时间投入到系统的模型建立上去,节省了工作者很多时间,提高了设计质量,相对于其他的仿真方法具有显著的优势[4-6]。

收稿日期:2015-11-30

基金项目:江西省研究生创新专项资金项目(YC2014-S246);江西省教育厅科技项目(GJJ14371)

作者简介:张利华(1972—),男,副教授,博士,研究方向为电气信息技术,通信网络信息安全。

1　基于模型的安全评估方法

1.1　安全评估模型标准

经过长期的铁路事业发展，在铁路技术安全领域，已经形成了一套安全标准，对铁路从产品研发到安全测试以及后来的维护维修都提供了有力的支持。铁路领域的一些标准及应用范围主要有[7]：

1）EN 50126 铁路应用：可靠性、可用性、可维护性和安全性（RAMS）规范和说明；

2）EN 50128 铁路应用：铁路控制和防护系统的软件；

3）EN 50129 铁路应用：铁路控制系统领域的安全相关电子系统；

4）EN 50159.1 铁路应用：通信、信号和处理系统（在封闭传输系统中与安全相关的通信）；

5）ENS 0121 铁路应用：电磁兼容。

1.2　铁路的 V 模型开发

铁路领域的安全评估工作主要遵循的是安全苛求系统开发 V 模型，具体如图 1 所示。

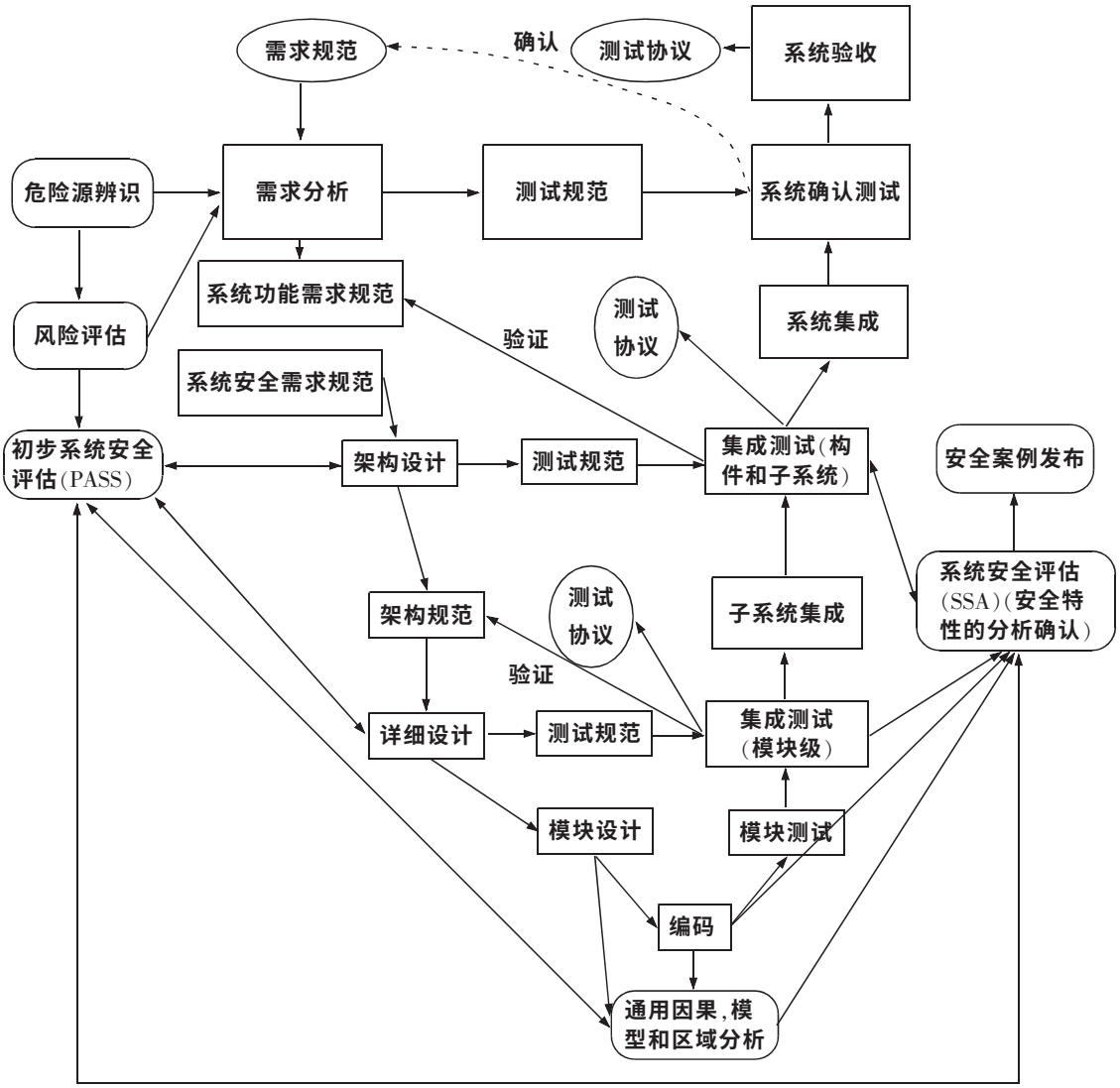

图 1　安全苛求系统开发 V 模型

Fig.1　V model of demanding security system development

1.3　安全评估方法

系统安全分析方法是安全分析结果科学性与合理性的重要保障，在系统的整个安全周期中，每个阶段

都有适用的分析方法。对系统隐患进行分析,思考的角度不同,对隐患源的分析思路也不同,使用的安全分析方法也不同。目前人们已经研究了数十种系统安全分析方法,适用于不同的分析过程,从分析的逻辑方法和角度可分为归纳法和演绎法,从分析的数理方法的角度可分为定性分析方法和定量分析方法。定性分析方法是定量分析方法的基础。

常用的几种传统安全分析方法主要包括安全检查表法,预先危险性分析法,故障模式等,各种方法对比如表1。

表1 主要安全评估方法列表

Tab.1 The list of main security assessment methods

方法	目的	适用范围	分析	优缺点
SCL	隐患识别及评价	系统的设计,制造,验证,运行,改造,拆除阶段	定性	全面,操作简单方便,易于掌握;编制检查表难度及工作量大
PHA	初步隐患识别,原因及影响分析	系统的设计,研发,制造,验证,改造阶段	定性	简单易行,受分析评价人员水平及主观因素影响较大
FFA	隐患识别及初步分析	系统的设计,研发,验证,改造阶段	定性	简单易行,受分析评价人员水平及主观因素影响较大
FMECA	隐患识别,原因及影响分析	系统的设计,验证,运行,改造阶段及事故调查	定性	容易掌握,有针对性,实用性强,但是需要评价人员对系统详细设计,设备功能及故障模式熟知,受人员水平及主观因素影响较大
FTA	隐患产生原因分析及发生概率计算	系统的设计,验证,运行,改造阶段及事故调查	定性 定量	复杂,工作量大,精确;故障树编制有误易失真
ETA	隐患潜在后果分析及事故概率计算	系统的事故验证,运行,改造阶段及事故调查	定性 定量	简便易行,受分析评价人员影响较大
HAZOP	系统偏差分析及原因,影响分析	系统的设计,验证,运行,改造阶段及事故调查	定性 定量	简便易行,受分析评价人员影响较大

SIMFIA是一个非常强大的安全评估仿真软件工具,能够提供各种各样的方法选择,在本次安全仿真中,主要通过对模型进行故障树分析,求出临时限速服务器出现故障的最小割集。

2 临时限速服务器结构

高速铁路信号系统主要由地面设备和车载设备组成。地面设备主要有:列控中心(TCC),调度集中(CTC),无线闭塞中心(RBC),计算机联锁(CBI),轨道电路、临时限速服务器(TSRS),无线通信设备(GSM-R)等;车载设备主要包括:应答器接收模块(BTM),车载安全计算机(VC),GSM-R无线通信单元(RTU)等[8-9]。具体如图2所示。

TSRS是一个安全相关设备,是CTCS-3级列控系统中信号控制的重要组成部分,其设计严格遵循"故障-安全"原则以保证系统达到要求的可用性和安全性水平[10-11]。临时限速系统与CTC、TCC、RBC及相邻的TSRS等设备之间均有信息交互。调度中心主要通过3个步骤设置临时限速过程:第1,根据线路的实际情况,调度员通过临时限速操作终端,将全线的限速计划命令以图形化的方式拟定完毕,并交至CTC行调台的行调员,行调员确认限速命令,并送至TSRS存储;第2,TSRS对存储器里的计划限速命令不断的进行检查,判断是否有到达具体执行时间的限速命令,若有,则送到临时限速操作终端并提示激活信息,由调度员对提示信息进行确认;第3,调度员确认后,根据具体时间,激活限速命令,激活后的限速命

令通过安全数据网传送给 TCC 和 RBC 校验、执行等，临时限速命令的设置和取消均采用双重口令用来保证信息交互过程的准确性[12-13]。

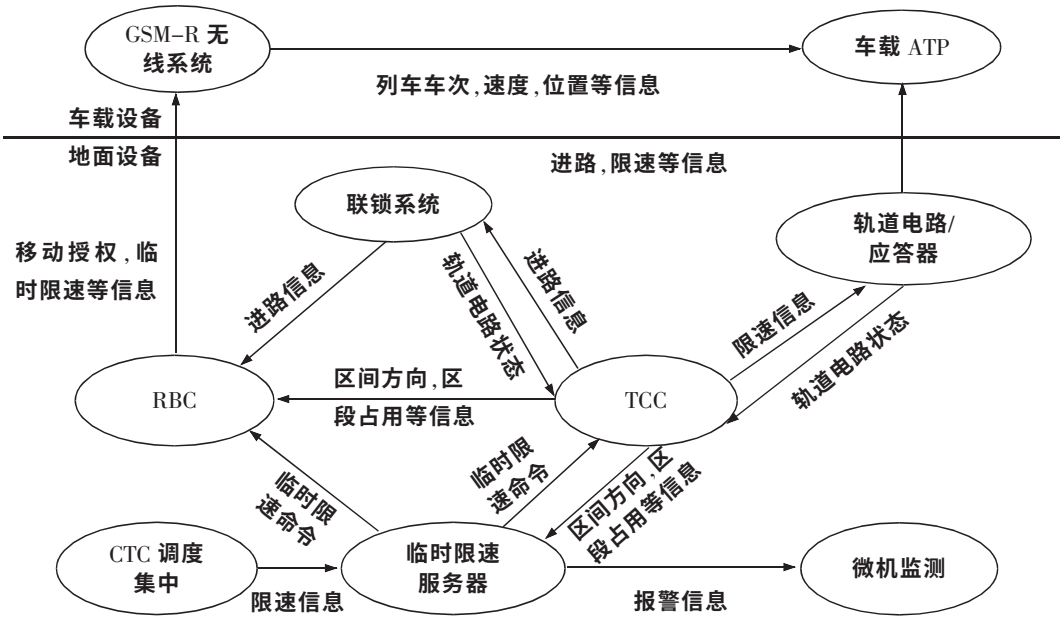

图 2　列控系统结构图

Fig.2　The structure of train control system

3　临时限速服务器 SIMFIA 建模流程

SIMFIA 建模方式灵活，可自上而下展开模型，也可自下而上集成模型。通过设置各个组件模块之间的逻辑关系，建立系统仿真模型，再利用 SIMFIA 强大的故障分析能力，自动生成故障树，从而实现准确的安全评估。建模采用自下而上建模方式按照以下几个步骤进行展开。

3.1　抽象化模型

使用 SIMFIA 软件对系统进行建模仿真，首先需要对评估对象进行抽象化。主要内容为对临时限速服务器的功能、层次、结构和输入输出进行抽象化，使之尽可能的反映真实系统的各方面情况。为此共建立了调度员、CTC、相邻 TSRS、TSRS、以太网、维修终端、维修人员、TCC、RBC、车载设备几个模块。其中考虑到真实系统全部为双倍冗余结构，在每个模块内部都包含了两个功能相同的子模块。例如 TSRS 模块中封装了 TSRS_1 和 TSRS_2 两个子模块。

3.2　建立故障模型

使用 SIMFIA 对抽象化的临时限速服务器模型进行绘制，定义模型中各模块的逻辑连接和失效模式。并在考虑了元件（系统）的正常工作模式下，对模型的失效状态进行扩展。在本次建模中，所有模块的失效模式皆为正常和失效 2 种。

3.3　验证模型

完成模型的描绘和逻辑关系的连接设置后，需要对模型的准确性进行验证。主要是验证模型的正确性、完整性、一致性。完整性指的是建立的模型是否完整，一致性指每个模块建模标准是否一致，正确性指建立的模型是否能正确反映系统的工作过程。通过对模块注入故障验证模型的故障传递过程，结果符合临时限速服务器的真实工作过程。具体模型如图 3 所示。在模型中，黑色圆圈表示输出，白色圆圈表示输入，四边形表示功能模块。

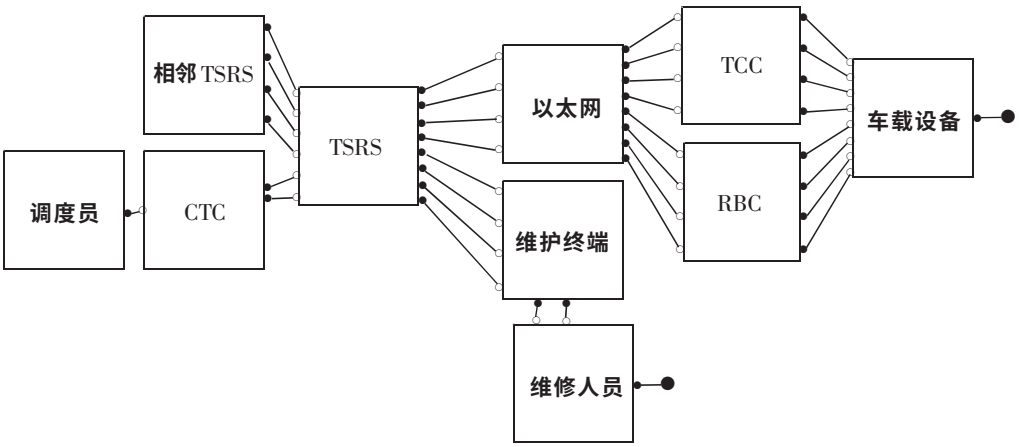

图3 临时限速服务器建模仿真图

Fig3. Temporary speed limit server modeling and simulation

SIMFIA建模方式灵活,可自上而下展开模型,也可自下而上集成模型。通过设置各个组件模块之间的逻辑关系,建立系统仿真模型,再利用SIMFIA强大的故障分析能力,自动生成故障树,从而实现准确的安全评估。

4 评估结果分析

根据建立的系统模型,选择一些灾难性或者影响重大的失效事件生成故障树,再进行失效分析。SIMFIA只需要经过简单设置便能对任一节点故障树和故障概率进行自动生成的计算。选择顶事件"TSRS_1模块失效"生成故障树图如图4所示。

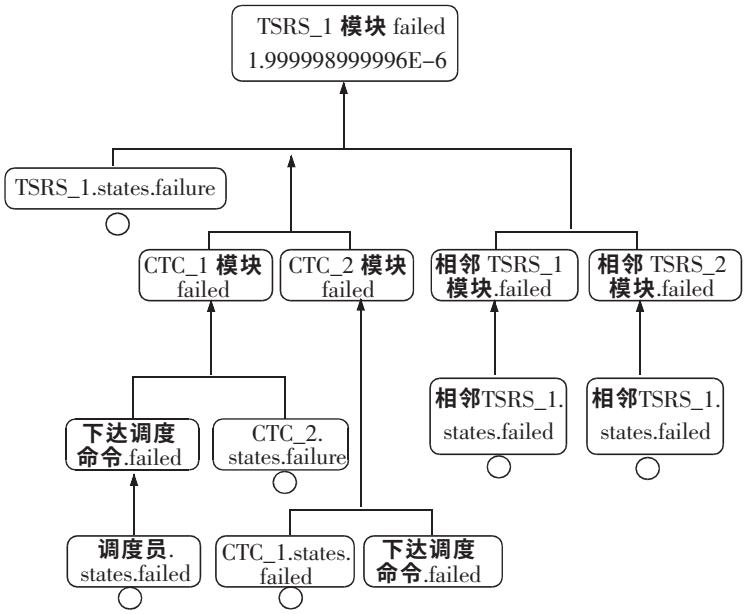

图4 临时限速服务器失效故障树图

Fig4. TSRS failure fault tree

图4中,事件下面有圆圈的表示该事件为顶事件失效的最小割集,三角形表示为同一事件。从图中可以看出顶事件TSRS_1模块失效的原因可能来自于工作中的每个途径,并最终识别出导致失效的原始原因为

调度员失效、CTC_1 失效、CTC_2 失效、相邻 TSRS_1 失效、相邻 TSRS_2 失效、TSRS_1 失效的一种或者多种。假设每个功能模块的故障率为 1e-6，计算 TSRS_1 模块连续工作 100 h 发生故障的概率为 1.999 998 999 996e-6。上述过程中，如果系统设计发生变化，只需要重新生成故障树即可，大大节省了计算时间。

5　结论

通过使用形式化建模方法对临时限速服务器进行安全性分析，我们可以得出以下结论有：

1）“TSRS_1 模块失效”发生的原因是最小割集中的一种或者多种发生导致，而且发生的概率为 1.999 998 999 996e-6，一般来说最小割集越少，系统安全性越高。

2）可以根据故障发生的概率调整修理周期，并在临时限速服务器发生故障时快速定位出故障源，找到故障传播的途径。

3）SIMFIA 软件与其他传统故障树分析方法相比较，具有操作简单，层次清晰等优点。

参考文献：

[1] 赵荣亮. 列控系统 TSRS 形式化建模分析与验证[D]. 重庆：西南交通大学，2014.
[2] 万勇兵，徐中伟，梅萌. CTCS-3 级列控系统临时限速服务器建模与形式化验证[J]. 系统仿真学报，2013，25(1)：132-138.
[3] 熊迎. 基于 UML 的客运专线列控系统临时限速服务器维护终端的研究与实现[D]. 北京：北京交通大学，2012.
[4] 邢逆舟，王立松. 基于模型驱动的航电系统安全性分析[J]. 计算机与现代化，2015(1)：21-26.
[5] 谷青范，王国庆，张丽花，等. 基于模型驱动的航电系统安全性分析技术研究[J]. 计算机科学，2015，42(3)：124-127.
[6] 张福凯，贺轶斐，谷青范. 基于模型驱动的 HUD 系统安全性分析方法研究[J]. 航空电子技术，2014，45(3)：52-56.
[7] 唐涛，徐田华，赵林. 列车运行控制系统规范建模与验证[M]. 北京：中国铁道出版社，2010.
[8] 聂超. CTCS-3 列控无线闭塞中心研究与仿真[D]. 重庆：西南交通大学，2010.
[9] 袁磊，王俊峰，康仁伟，等. CTCS-3 级列控系统临时限速建模与验证[J]. 西南交通大学学报，2013，48(4)：708-714.
[10] 邓紫阳. 基于着色 Petri 网 CTCS-3 级列控中心建模与仿真研究[D]. 北京：北京交通大学，2009.
[11] 易承龙. 基于 Simulink/Stateflow 的 CTCS-3 级列控系统建模与仿真分析[D]. 北京：北京交通大学，2014.
[12] 张爱玲. CTCS-3 级列控系统 RBC 行车许可生成的形式化建模与分析[D]. 兰州：兰州交通大学，2012.
[13] 秦舒，毛鑫，沈钢. 基于 simulink/stateflow 的列车碰撞时钩缓系统建模[J]. 华东交通大学学报，2015，32(1)：22-26.

Security Assessment of Temporary Speed Restriction Server

Zhang Lihua , Luo Zhihua

(School of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: In recent years, with China's rapid development of high speed railways, more and more high speed railway lines have been put into operation effectively, alleviating the pressure on China's railway travel. But frequent railway accidents have caused great threat to people's life and property security. It is urgent to probe into how to ensure the safe operation of the railway. Temporary speed restriction server is an important part of CTCS-3 train control system whose safety directly affects the safe operation of high-speed railway. Combined with the actual operation of the temporary speed restriction server process, by use of the security analysis software - SIMFIA to build simulation model of temporary speed restriction server, this study automatically generated the fault tree of the system, and calculated the minimal cut sets of the failed state. According to the fact that minimum cut sets can quickly find fault source, it analyzed the security of temporary speed restriction server.

Key words: temporary speed restriction server; security assessment; minimum cut set; SIMFIA; modeling and simulation

（责任编辑　姜红贵）