文章编号：1005-8451（2015）05-0053-05

城轨CBTC系统联锁表数据安全逻辑验证方法研究

张　淼，黄友能，任啸宇
（北京交通大学　轨道交通控制与安全国家重点实验室，北京　100044）

摘　要：联锁表是联锁安全逻辑的体现，本文针对联锁表数据的安全逻辑验证问题，提出一种基于CSP的验证方法。首先对联锁表数据进行建模，将联锁表数据抽象为调度员、道岔、信号机、区段和联锁控制器5个进程的并发组合模型，并对各进程进行建模。依据联锁系统安全约束条件，从功能性和安全性两个方面，通过对模型正确性的验证来说明数据的安全逻辑正确性。最后以北京地铁亦庄站联锁表数据的安全逻辑验证为例，说明该方法的可行性。

关键词：CBTC；联锁表逻辑；CSP
中图分类号：U132.7：TP39　**文献标识码：**A

Data safety logic verification method of interlock table for Urban Transit CBTC System

ZHANG Miao, HUANG Youneng, REN Xiaoyu
(State Key Laboratory of Railway Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The interlock safety logic was reflected by interlock table. This paper proposed a verification method based on CSP (Communicating Sequential Processes) to solve the data safety logic verification problem of interlock table, modeled data of the interlock table at first, abstracted five processes of dispatchers, switch, signal machine, segment and interlocking controller from the data of interlocking table, and further modeled the processes respectively. The correctness of the model was verified from the functional and safety aspects. At last, an example of data safety logic verification with the interlock table in Yi Zhuang Station of Beijing Metro illustrated the feasibility of the method.

Key words: Communication Based Train Control(CBTC); interlock table logic; Communicating Sequential Processes(CSP)

基于无线通信的列车自动控制系统（CBTC）是保证列车安全运行的关键系统。计算机联锁设备作为该系统中一个重要的组成部分，主要实现站台和道岔区段信号机、道岔和进路之间的转换与解锁。

联锁表用来在车站和车辆段之间实现联锁关系，建立进路，控制道岔的转换，信号机的开放以及进路解锁，从而保证行车安全[1]。目前主要通过人工和功能测试的方法来保证联锁表数据安全逻辑的正确性，对人工和功能测试案例都提出了较高要求。

本文运用统一建模语言（UML，Unified Modeling Language，）对联锁表逻辑进行分析，将其抽象为对象及对象之间的信息交互过程，选取通信顺序进程（CSP）形式化语言[2]描述对象的状态转移关系，利用这种方法自身底层的数学理论支持，对所有节点可以全部遍历的优势，以北京地铁亦庄站为例，提出一种基于形式化的联锁表安全逻辑验证方法。

收稿日期：2014-10-19
基金项目：北京市科委项目（KWH13001531）；轨道交通北京实验室项目（W13H100061）。
作者简介：张　淼，在读硕士研究生；黄友能，副教授。

1　CSP定义及特点

CSP语法中，具体刻画某一客体相关全体事件名称的集合叫做这个客体的字母表，用进程代表客体的行为，并规定这些客体的行为是能用组成客体字母表的事件的有限集合来说明的。对象状态的转移实质就是行为的树状示意图中树根到该节点沿途遇到的标记序列。

CSP是一种研究与并发性相关的理论问题的优秀工具，它可以提供并发系统的形式化研究所需的所有机制[3]。作为一种形式化方法，不仅形象直观而且有数学理论支持，侧重研究系统间的交互通信，具有遍历节点的验证特性，能全面证明联锁表数据的安全逻辑。本文着重分析联锁表安全逻辑，用UML分析5个对象的交互关系，重点阐述联锁表逻辑的形式化建模与验证方法。主要研究路线如图1所示。

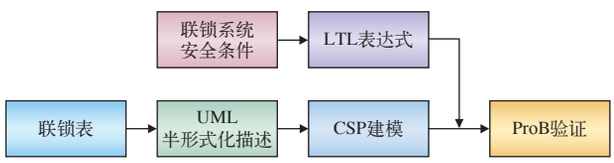

图1　主要研究路线

2　联锁表安全逻辑建模与验证

2.1　联锁表中的联锁逻辑

联锁表包含进路、信号机、道岔及区段等信息，从进路选排到进路防护信号机开放主要经过操作、选路、道岔转动、进路锁闭和信号开放5个阶段。

具体以北京地铁亦庄站典型道岔区段为例，列车进路F4～F6如图2所示。

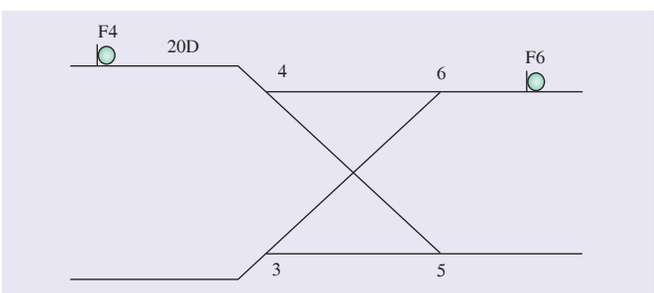

图2　F4～F6进路示意图

对应以上进路的联锁表信息如表1所示。

表1　亦庄站部分联锁表

站名	进路	进路性质	信号机		道岔	敌对进路	轨道区段	
			名称	显示			后备模式	CBTC模式
亦庄站	F4～F6	列车进路	F4	U	3/6，4/5	F6		20 G

由表1可知，在CBTC模式下，选择进路F4～F6，在满足逻辑区段20G空闲的状态条件下，检查道岔位置3/6，4/5是否为定位，若不是则转换道岔以满足要求；确定道岔状态后，检查敌对进路F6没有建立；则允许开放信号机F4，保持并开放进路。

2.2　UML顺序图描述联锁表逻辑信息

2.2.1　UML顺序图介绍

顺序图主要用二维图来描述系统运行时各对象之间的交互时序关系，可以实现用例的逻辑建模。主要由4个标记符构成：对象、生命线、消息和激活。纵向是时间轴，时间沿着生命线向下延伸，横向则代表参与相互作用的对象。消息由一个对象的生命线指向另一个对象的生命线的直线箭头来表示，上面注明发送的消息名。

2.2.2　联锁表逻辑的UML顺序图模型

由2.1联锁表逻辑过程分析，可以将参与联锁表逻辑的对象抽象为：调度员、道岔、信号机、区段和联锁控制器；对象之间的逻辑关系由系统对象间交互信息来表达。这样就可以将联锁表安全逻辑转化成在满足约束条件关系的前提下进行状态转移的关系。

具体到亦庄站的例子，用USER、SWITCH、F2、TRACK和CI分别表示系统对象，对象间消息的传递通道定义得到联锁表对象间的交互关系，用UML顺序图[4]形象直观地表达，如图3所示。

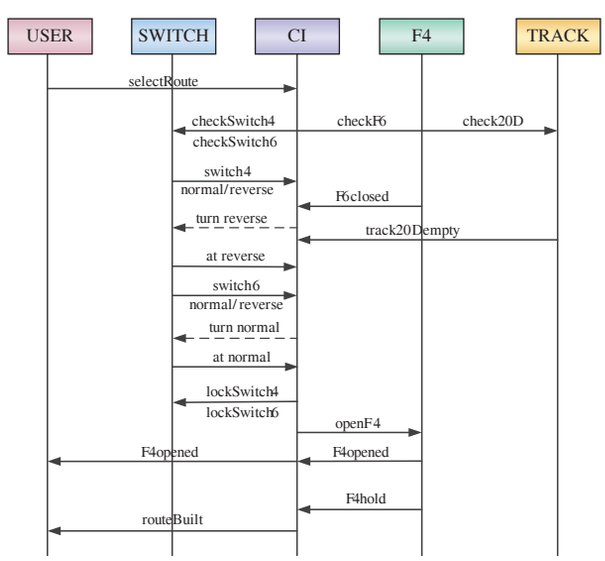

图3　进程F4-F6内部的消息传递示意图

2.3　联锁表逻辑的CSP模型及验证

在用CSP对系统建模过程中，将每个对象的操作称为一个进程。因此联锁表逻辑被看作5个进程间的并发交互过程。对象之间需要通过通道进行信

息交互，状态转换用基于 CSP 语义模型 [5] 中的迹图表示。

2.3.1　联锁表逻辑的模型化

联锁表逻辑可以表达成 5 个对象之间的信息交互过程。下面分别对不同对象的动作进行分析，并用 CSP 对其建模。

首先分析 USER 进程，调度员通过 chU2C 发送选择进路的命令给 CI，满足信号开放的条件后，CI 通过 ch_{C2U} 反馈给调度信号机 F4 开放和进路建立成功的消息。其 CSP 的迹模型如图 4 左侧所示。

USER=ch_{U2C}!selectRoute->ch_{C2U}?F4opened->ch_{C2U}?routeBuilt->USER

同理对于信号机 F4 来说，接收到联锁控制器发来的 openF4 信息后开放信号机，继而通过 ch_{S2R} 通道将状态信息反馈给 CI 进程。F4 进程的 CSP 语义描述为：

F4 = ch_{R2S}?openF4->ch_{S2R}!F4opened->ch_{R2S}?F4hold->F4

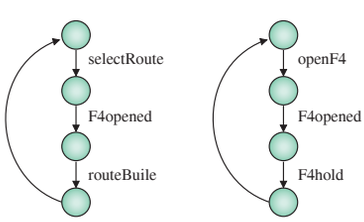

图4　USER和信号机F4进程迹图

SWITCH 进程通过 ch_{C2S} 通道收到联锁检查 4 号道岔和 6 号道岔的要求，操作过程中并不关注具体的时序关系，所以将道岔分别处理并看作两个进程，只有当这两个进程都满足条件时才能开放进路。在 CSP 中可以用并发来表达严格同步的两事件构成整个系统的行为，并同时参与到公共事件上。

这里对 4 号道岔的检查作如下说明，如果其位于正位，直接锁闭；若位于反位，则将其扳至正位，再进行锁闭，这之间是选择的关系，只有道岔锁闭后才能允许信号机 F4 开放。

SWITCH4=ch_{C2S}?checkSwitch4->(ch_{S2C}!normal->ch_{C2S}?lockSwitch4)[](ch_{S2C}!reverse->ch_{C2S}?turnSwitch4->ch_{S2C}!normal->ch_{C2S}?lockSwitch4)->openF4->SWITCH4

同理对于 6 号道岔的检查、操作与锁闭用 CSP 代码表达如下：

SWITCH6=ch_{C2S}?checkSwitch6->(ch_{S2C}!normal->ch_{C2S}?lockSwitch6)[](ch_{S2C}!reverse->ch_{C2S}?turnSwitch6->ch_{S2C}!normal->ch_{C2S}?lockSwitch6)->openF4->SWITCH6

只有当上述两个进程进行到公共事件，openF4 才可以发生，满足案例的实际需求，道岔进程的 CSP 最终表达式如下：

SWITCH= SWITCH4|| SWITCH6

对应迹图如图 5 所示。

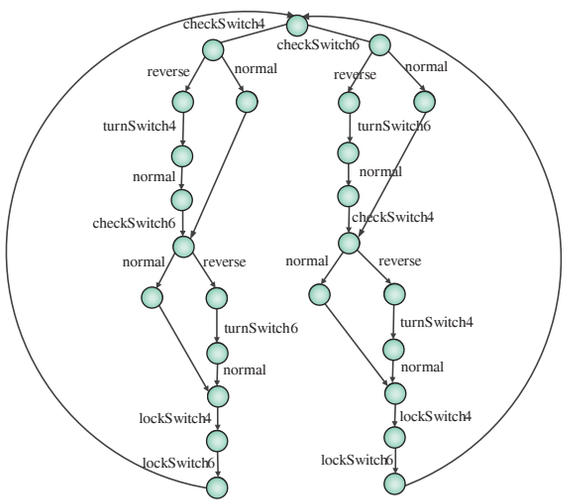

图5　SWITCH进程迹图

道岔锁闭之后，要对区段出清以及敌对进路未建立做进一步的确认。这就要对 Track20D 对象进行分析建模。Track20D 通过 ch_{C2S} 通道接收联锁控制器发来的检查轨道区段状态的命令，分别检查 20D 是否空闲以及敌对信号 F6 是否开放，对应的 CSP 模型表达如下：

Track20D=ch_{C2S}?check20D->ch_{T2C}!-track20Dempty->Track20D)[](ch_{T2C}!track-20Doccupied → STOP)

F6=ch_{C2S}?checkF6->(ch_{T2C}!F6closed->F6)(ch_{T2C}!F6open->STOP)

TRACK= Track20D||F6

基于 CSP 语义模型中的迹模型，进程 TRACK 的迹模型如图 6 所示。

控制器作为最复杂的元件和系统中所有对象之间都存在交互关系，从时间的先后进行角度，首先 CI 进程由通道 ch_{U2C} 收到调度员发出的选排路指令，如果符合道岔锁闭在正确位置、区段空闲且不存在

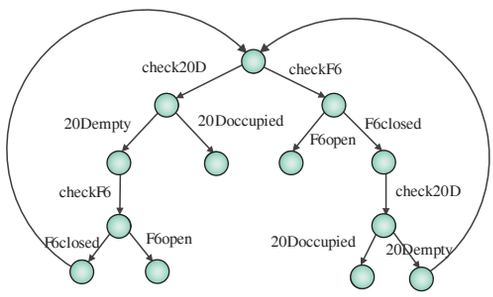

图6　TRACK进程迹图

敌对进路的条件则开放信号机，若其中一个条件不满足，则进路无法建立。用 CSP 迹图形象直观的表达上述建立进路的联锁逻辑信息，图 7 为先对道岔 4 位置检查的联锁控制器进程迹图。

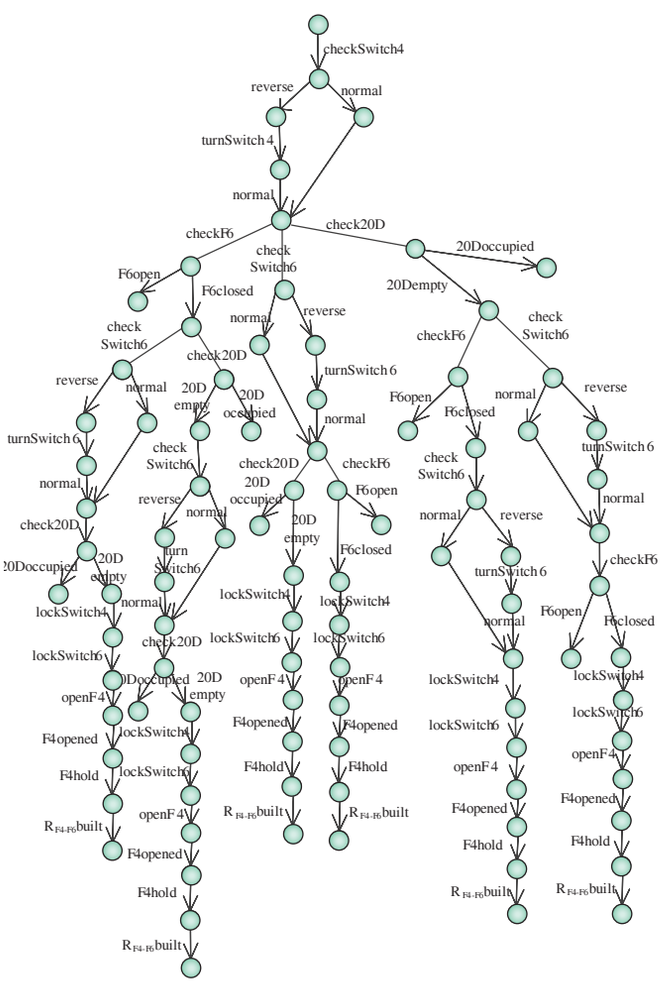

图7　CI部分进程迹图

综上所述，进路 F4 ～ F6 的行为就是 5 个对象的行为的并发组合：

F4-F6=USER||SWITCH||F4||TRACK||CI

联锁表由多条进路组成，每一条进路都可仿照上述思想建立模型，最终所有进路的并发组合就作为联锁表逻辑的完整模型，通过对模型正确性的验证来说明数据的安全逻辑正确性。

2.3.2　模型的验证

计算机联锁表逻辑是行车最基础的安全保证。从总体验证思路上，将联锁表逻辑的验证分为功能性验证和安全性验证，所谓安全性验证，主要是满足列控领域相关要求的特殊属性。

建模及验证工具 ProB[6] 为联锁逻辑提供针对不同性质便捷的模型验证技术，像死锁、活锁，可达性，线性时序逻辑（LTL，linear temporal logic）[7]，优化验证和可能性模型验证，此工具通过深度和广度优先搜索，遍历模型中所有状态节点，以快速找出存在问题节点的最短路径。

（1）功能性验证

功能性验证主要是从模型性质的角度对系统进行验证，保证所有节点的状态转移

#assert System() deadlockfree;

死锁状态是指无法成功终止一个不可动的状态。

#assert System() divergencefree;

活锁状态是指给定一个进程，它一直在内部转换，无法到达有用的事件。

#assert System() deterministic;

确定性是指给定一个进程，如果它是确定性的，那么不论任何状态，一个事件不会迁移到两个状态。

（2）安全性验证

联锁作为安全苛求系统，其中联锁表的安全逻辑反应了系统的可靠性和安全性，是安全性验证的重点。在进路建立的过程中，主要关注以下 3 方面：进路道岔及防护道岔被锁闭；进路区段空闲且解锁；敌对进路未建立。用 LTL 语言来描述进路需要满足的安全条件。

a. 验证当进路上所有道岔位置正确且锁闭时进路才能建立，针对 F4 ～ F6 进路，即当道岔 4、道岔 6 分别在定位且锁闭时进路建立，信号机 F4 才能开放。对应 LTL 表达式：

G([switch4normal]&[switch6normal]=>F[F4opened])

b. 验证进路对应区段空闲才能建立进路，进路

（下转 P60）

信息发送组合策略（滚动消息高级覆盖低级、同级叠加，紧急消息高级覆盖低级、同级发送最新消息）进行消息调度，消息调度完成后，发送播放器终端，由终端设备显示输出。

3 结束语

PIS 作为城市轨道交通运营的重要系统之一，在地铁运营中发挥着乘客信息引导服务的重要作用。本文分析了当前 PIS 设备管理的业务需求，设计了软件功能，并对系统架构设计进行分析。为实现 PIS 降级模式下的业务功能要求，保证在中心、车站网络故障情况下，车站系统对设备的有效控制和运营信息发送，系统采用中心部署数据库、车站以同步文件方式访问系统，以较低的成本和简单的部署结构解决了中心－车站两级系统间数据一致性的难点。

随着物联网技术的深入发展以及地铁运营商对地铁各弱电系统状态监视及统一控制要求越来越高，未来一段时间内，需要借助电子、网络、传感等新技术对 PIS 各级设备的更多参数信息进行采集，并对设备的工作状态进行智能监视和控制，为设备的稳定和可靠运行提供更多保障。

参考文献：

[1] 吴闯龙 . 城市轨道交通乘客信息系统的发展 [J]. 铁路通信信号工程技术，2007，4（5）：46-48.

[2] 曾　娜，许　昆，李　军 . 轨道交通乘客信息系统的设计 [J]. 总线与网络，2011 (6)：12-15.

责任编辑　陈　蓉

（上接 P56）

F4 ～ F6 要检查的区段是 20D，相应的 LTL 表达式：

G([track20Dempty]=>F[F4opened])

c. 要验证任意两条敌对进路不能同时建立，容易从联锁表中找到进路 F4 ～ F6 的敌对进路信号为 F6，将关系写成 LTL 表达式：

notG([F4opened]&[F6open])

在 ProB 中将联锁表中每一条进路按上述安全条件列举，逐项验证性质，得到的结果中若没有反例以证明模型的安全性，从而通过证明模型的正确性追溯到联锁表数据安全逻辑的正确性。

（3）结果分析

将亦庄站的联锁表中列车进路部分的每一条进路写成 5 个对象之间的交互关系，继而对所有进路用 CSP 建模，录入到模型验证工具 ProB 中。选择 Verify->Model Check，利用自动验证判断出模型自身无死锁、活锁且满足确定性断言。

在 ProB 中对道岔位置、逻辑区段空闲和敌对进路建立的安全条件逐条检测，验证结果没有反例，说明模型中任意两条敌对进路都无法建立；进路的道岔与进路开通方向一致且锁闭，满足逻辑区段空闲条件时，才可能建立，从而得到安全性方面的模型验证结果，综合得出亦庄站的联锁表数据逻辑满足安全性要求的结论。

3 结束语

本文以北京地铁亦庄站列车进路联锁表数据为例，用 CSP 定义联锁表安全逻辑的具体过程。联锁表数据安全逻辑 CSP 模型的应用显示，该模型不仅能模型化系统对象间的交互过程，还能对联锁系统安全性和实时性进行分析，保证联锁表安全逻辑的正确性。

参考文献：

[1] 宿浩峰 . 城市轨道交通联锁系统建模的研究 [D]. 杭州：浙江大学，2012.

[2] C.A.R.Hoare.Communicating Sequential Processes[Z]. Prentice Hall, Inc., Upper Saddle River, NJ, USA, 1985.

[3] 孙　麒，张云华 . 基于 CSP 的形式化方法研究 [J]. 浙江理工大学学报，2009，26（4）：557-560.

[4] 程　梁 . 基于 UML 的联锁软件建模与仿真研究 [D]. 北京：北京交通大学，2007.

[5] 屈延文 . 形式语义学基础与形式说明 [M]. 北京：科学出版社，2009：418-466.

[6] Michael Leuschel, Michael Butler. ProB: A Model Checker for B[D]. Department of Electronics and Computer Science, University of Southampton, 2014.

[7] 赵岭忠，张　超，等 . 基于 ASP 的 CSP 并发系统验证研究 [J]. 计算机科学，2012，39（12）：125-132.

责任编辑　陈　蓉