doi:10.11835/j.issn.1000.582X.2023.09.012

CTCS-3级列控车载设备的形式化建模与验证

何 涛[a,b],韩敬佳[a]
(兰州交通大学 a.自动化与电气工程学院;b.甘肃省工业交通自动化工程技术研究中心,兰州 730070)

摘要:CTCS-3级列控系统安全苛求性较高,而列控车载设备是CTCS-3级列控系统的主体,主要功能是对列车进行操纵和控制,保证列车安全运行的关键。通过分析CTCS-3级列控车载设备之间的信息交互以及车载安全计算机中工作模式的转换规则,采用有色Petri网(CPN)建立车载设备的信息交互模型以及工作模式转换模型,使用ASK-CTL分支时序逻辑公式验证了模型的死标识、死锁以及分析工作模式下的系统行为等特性,验证构建的CPN模型符合系统规范要求的流程及规则,可为相关安全苛求系统的设计提供一定参考。

关键词:列控系统;车载设备;模式转换;有色Petri网
中图分类号:TP391;U284 **文献标志码:**A **文章编号:**1000-582X(2023)09-120-10

Formal modeling and verification of CTCS-3 train control on-board equipment

HE Tao[a,b], *HAN Jingjia*[a]
(a. School of Automation and Electrical Engineering; b. Gansu Research Center of Automation Engineering Technology for Industry &Transportation, Lanzhou JiaoTong University, Lanzhou 730070, P. R. China)

Abstract: The CTCS-3 train control system is subject to stringent safety requirements, with the train control on-board equipment serving as its core. This equipment plays a vital role in operating and controlling the train, ensuring the overall safety of train operation. In this study, the information interaction between CTCS-3 train control on-board devices and the work mode conversion rules in the on-boar safety computer was analyzed. To establish a comprehensive model, colored Petri nets (CPN) were used, enabling the construction of an information interaction model and work mode transformation model for the on-board equipment. To validate the model's effectiveness, the ASK-CTL branching sequence logic formula was used to verify its performance concerning dead identification, deadlock and transferability under various working modes. The results show that the CPN model conforms to the system specification requirements, adhering to the expected process and rules. This research provides valuable ingishgts and serves as a reference for the design of the relevant security demanding systems.

Keywords: train control system; on-board equipment; mode conversion; colored Petri net

收稿日期:2020-06-09
基金项目:国家自然科学基金资助项目(U2268206)。
Supported by National Natural Science Foundation of China(U2268206).
作者简介:何涛(1977—),男,教授,硕导,主要从事轨道交通测试研究方向研究。
通信作者:韩敬佳(1994—),女,硕士,主要从事列控系统建模分析方向研究,(E-mail)1558155326@qq.com。

近年来，中国对于时速超过250 km/h的铁路采用的是CTCS-3级列车运行控制系统（以下简称C3级列控系统）[1]，车载设备是C3级列控系统的重要组成部分，其安全性、可靠性直接影响列车运行安全。因此对列控车载设备进行建模，验证车载设备系统功能及转换流程满足相关系统需求规范，对保证列车运行安全，改进系统需求规范具有重要意义。

目前，国内外对Petri网的运用以及对列控系统的建模与仿真做了许多研究，德国学者Hardi[2]以现有的ERTMS/ETCS规范为基础，采用着色Petri网（CPN）构建了形式化模型。应用一种集成的面向事件和数据的方法，显示系统在自己的Petri网层次上的不同方面。中国学者采用UML建模方法[3]，对CTCS-3级列控车载设备进行分析与建模，依据系统模型提出车载设备测试案例和测试序列设计。UML是一种半形式化建模方法，不能对构建的模型进行验证，具有一定局限性，给系统的验证和分析带来困难。另外还有时间自动机建模方法[4]可对CTCS-3级列控车载设备中的车载安全计算机VC和无线闭塞中心RBC进行建模，验证车载设备的系统特性。时间自动机是形式化建模方法，适合描述反应式系统，对于复杂系统，构造时间自动机模型的工作量比较大，不适合描述具有并发状态的系统。 C3级列控车载设备是对安全性要求较高的复杂系统。仅仅依靠传统建模语言无法完全描述出CTCS-3级列控车载设备模式转换的多样性，因此，需要一种能够描述复杂系统的建模语言对模式转换进行分层建模，能够更好表现系统的功能及结构。对比目前现有UML以及时间自动机等建模方法，Petri网有直观的图形表示，又可以引入数学方法对建立的模型进行验证与分析[5]。用有色Petri网CPN（colored petri net）建立模型完成后可以直接用工具CPNTools进行验证和分析，对于C3级列控系统这种复杂系统，可以对其进行分层描述来简化模型结构，减小系统验证复杂度。因此，选用有色Petri网更加适用于列控系统的建模，解决系统空间爆炸问题，更加适用于复杂系统的建模。

1　车载设备功能需求分析

CTCS-3级列控系统的主要功能有保障行车安全、保证运输效率、保证乘客舒适度等[6]。C3级列控系统主要由2部分组成：一部分是提供监控列车所需要的线路允许速度、行车许可等基础数据的地面设备；另一部分是根据相关设备传送上来的地面信息监控列车运行速度、运行条件的车载设备。

C3级列控车载设备是C3级列控系统的核心设备，采用故障-安全设计，车载设备主要构成有：主控单元车载安全计算机（VC）、GSM-R无线通信、轨道电路信息读取器（STM）、应答器信息接收单元（BTM）、列车接口单元（TIU）、人机界面（DMI）、等[7]。C3级列控车载设备构成如图1所示，其主要功能包括：

1）向RBC发送列车运行所需动态信息，处理来自车载的调车请求。

2）处理来自RBC的紧急停车消息，根据情况对列车实行控制命令。

3）接收无线闭塞中心RBC发送来的正常行车许可MA、列车位置报告等。

4）根据接收到的应答器信息，计算行车曲线及列车位置校正。

5）接收轨道电路传送的线路参数信息。

6）实时测量列车运行速度和行走距离并计算目标距离模式控制曲线。

7）RBC/RBC的交接。

8）DMI的管理、司法数据的记录功能。

车载安全计算机VC是C3级列控车载系统的控制核心，主要完成车载设备工作模式的判断及转换，根据从其他模块获取的信息，必要时对列车实施制动，以保证车载系统对列车安全防护功能的具体实现和操作。因此，选用车载安全计算机中工作模式转换作为车载设备安全计算机的主要状态。

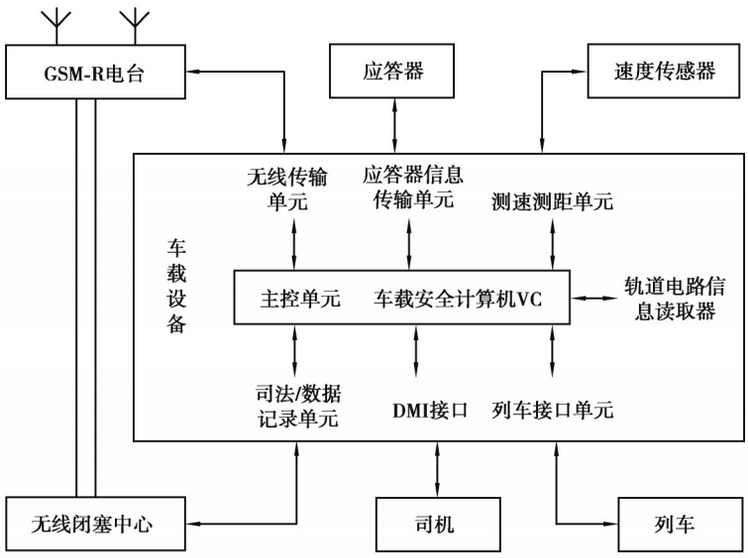

图 1 CTCS-3 级列控车载设备结构

Fig. 1 Structure of CTCS-3 train control on-board equipment

2 CPN 模型的构建

2.1 建模研究思路

根据有色 Petri 网建模语言的建模流程,将对车载设备的建模思想总体分为 3 部分:一是系统功能分析,根据系统规范了解车载设备间信息交互和车载设备中工作模式转换条件;二是根据系统功能构建 CPN 模型;三是根据系统属性对构建的模型进行验证。CTCS-3 级列控车载设备形式化建模与验证的总体框架图如图 2 所示。

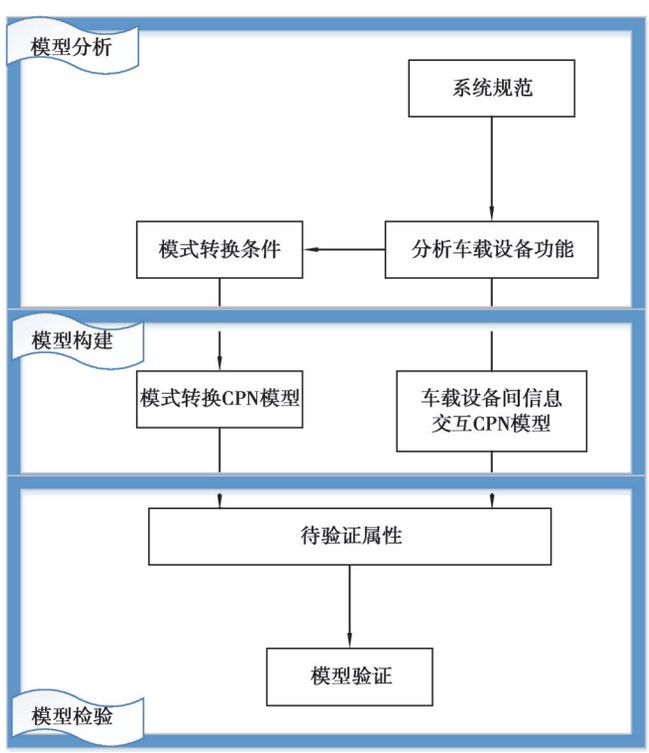

图 2 车载设备建模与验证框架图

Fig. 2 Block diagram of on-board equipment modeling and verification

具体建模流程如下：

1）根据《CTCS-3级列控系统需求规范（SRS）》[8]中的要求，采用有色Petri网对CTCS-3级列控系统车载设备各部分之间的信息交互以及车载安全计算机中工作模式转换进行建模。

2）基于有色Petri网构建出车载设备以及模式转换的CPN模型，其中对系统模型采用分层（2层）的构建规则，根据系统需求规范中的模式转换条件，将车载安全计算机设为替代变迁，它的子页模型为各模式之间的转换。

3）在CPN Tools工具中引入分支时序逻辑ASK-CTL公式对构建的CPN模型进行形式化验证，分析模型是否满足《CTCS-3级列控系统需求规范（SRS）》要求的车载设备信息交互功能以及模型是否符合车载设备模式转换流程，若不满足，则重新采用有色Petri网对车载设备进行建模。

4）在模型验证结果正确的基础上，分析系统的属性是否满足车载设备信息交互功能以及是否符合模式转换流程。

2.2　有色Petri网建模方法

有色Petri网是一种形式化的建模语言，与其他建模语言相比有色Petri网构建的CPN模型更加直观形象，还能对复杂系统进行分层建模来描述系统的功能和行为，大大简化系统模型的复杂度。CPN作为一种图形化的表达形式，主要由库所（P用圆表示，代表系统的状态）、变迁（T用矩形表示，代表系统状态的改变或动作的执行）、托肯（token代表数据类型）、有向弧（A用箭头表示，代表托肯的流动方向）组成。

ASK-CTL模型检验用于验证建模语言有色Petri网描述的系统模型与设计的系统性质是否一致。将系统需要验证的性质用ASK-CTL公式进行描述与验证，如果系统模型符合描述的验证语言则返回结果“true”，如果不满足则返回“false”，以便根据验证结果对设计进行修改[9]。

定义1　CPN = $(\sum, P, T, A, N, C, G, E, M_0)$，若 $M \in R(M_0)$，使 $\forall t \in T: \neg M[t>$，则称 M 是CPN的一个死标识（deadmarking）。

定义2　CPN = $(\sum, P, T, A, N, C, G, E, M_0)$，其中 $P_1 \in P$。若 ${}^*P_1 \subseteq P_1{}^*$，则称 P_1 为CPN的死锁（deadlock）。

基于ASK-CTL公式的模型验证算法如图3所示。

在CPN Tools中对系统模型进行检测时常用的函数是eval_node()，函数的格式是：val eval_node(VALUE self, NODE* node)，其中self是ASK-CTL库中自带的查询函数[10]，例如自循环终端的检测常用OutNodes()函数，当返回结果为“There is No loop Terminal!”时，表示系统模型不存在自循环；死锁的检测常用InvalidTerminal()函数，当返回结果为“No Deadlock Markings!”时，表示系统模型不存在死锁。

```
Input: CPN model
Step1: Get the State Space Report from the CPN model by
       using CPNTools                          //得到状态空间仿真报告
Step2: While((Home&&Boundness&&Fairness)=1)
       do  if(Liveness!=1)                     //CPN中存在死标识
           go to Step3;
           else Step7;
Step3: ListDeadMarkings();                     //枚举死标识
       if(OGNodes.num==SCCGNodes.num  //活锁检测
           go to Step4;
           else Step7;
Step4: SelfloopTerminal n=(OutNodes(n)=[n]); //自循环终端检测
       InvalidTerminal();                      //无效终端检测
       if(TextIO.output=" No Selfloop Terminal")
           go to Step5
           else Step7
Step5: VaildTerminal();                        //死锁检测
       InvalidTerminal();
       if(TextIO.output=" No DeadLock Markings!")
           go to Step6
           else Step7
Step6: The Dead Markings are Reasonable!
Step7: The Dead Markings are Unreasonable!
```

图3　基于ASK-CTL公式的模型验证算法

Fig. 3　Model validation algorithm based on the ASK-CTL formula

2.3　构建车载设备CPN模型

C3级列控车载设备是对安全性要求较高的复杂系统。仅仅依靠传统的建模语言无法完全描述出CTCS-3级列控车载设备模式转换的多样性，因此，需要一种能够描述复杂系统的建模语言对模式转换进行分层建模，能够更好表现出系统功能及结构。

C3级列控车载设备中的核心设备是车载安全计算机，保证车载系统对列车安全防护功能的具体实现和操作[11]。车载安全计算机主要实现车载设备工作模式的判断及转换，实现列车基本运营场景；RBC收到来自车载的行车许可MA请求和列车位置报告（train position）后，根据相关信息计算生成行车许可MA，并将临时限速信息、线路信息等通过GSM-R发送给安全计算机用以生成速度控制曲线；考虑司机对列车运行状态的

影响,司机的主要状态是确认安全计算机传来的信息,必要时对列车实施人工制动;列车的主要状态是向安全计算机提供列车速度及位置信息后接收安全计算机发送的对列车控制要求以及制动命令;应答器主要是用于列车定位,应答器发送的线路参数、临时限速等信息主要是为了满足C3级列控系统后备模式C2级列控系统的控制,但RBC切换、级间转换等信息是利用地面应答器发送的。根据系统需求规范中提出的车载设备和司机相关职责构建出车载设备之间信息交互CPN模型如图4所示。

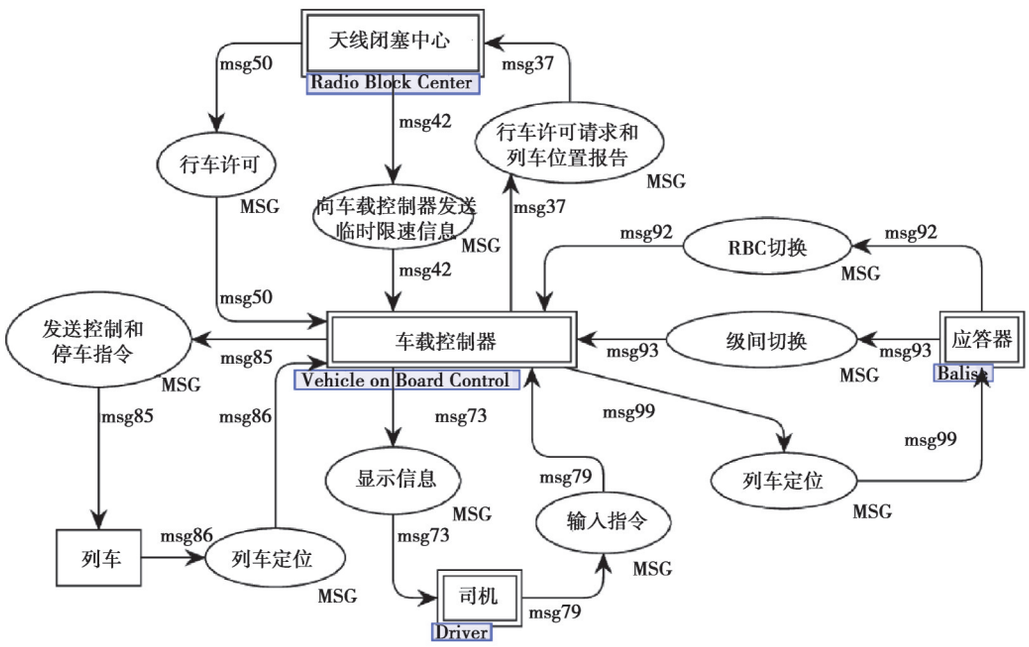

图4 车载设备间信息交互CPN模型

Fig. 4 CPN model of information interaction between vehicle devices

CPN模型以车载安全计算机为中心,车载设备主要变迁设为RBC、司机、列车、应答器,将其与车载安全计算机的信息交互设为CPN模型的系统状态即库所,根据车载设备的功能可知库所的主要状态如表1所示。

表1 库所主要状态说明

Table 1 Description of the main state of the place

变迁	库所状态	颜色集	含义
RBC	MA	msg50	行车许可
	Issuing TSR Order to VOBC	msg42	向VOBC发送TSR指令
	MA Request and Train Position	msg37	向RBC发送MA请求和列车位置报告
Driver	Input Order	msg79	向VOBC发送输入指令
	Display Info	msg73	显示信息
Train	Train Position	msg86	列车位置信息
	Send Control and Brake Command	msg85	发送控制和停车指令
Balise	RBC Handover	msg92	RBC切换
	Level Conversion	msg93	级间转换
	Train Position	msg99	列车定位

车载设备的工作过程由工作模式不断转换来实现,因此将模式转换作为安全计算机的主要状态进行建模。CTCS-3级列控车载设备主要包括待机模式(SB)、完全监控模式(FS)、调车模式(SH)、目视行车模式

（OS）、引导模式（CO）、休眠模式（SL）、冒进防护模式（TR）、冒进后防护模式（PT）、隔离模式（IS）9种工作模式[12]。系统需求规范中规定了各工作模式转换之间的转换条件。车载设备工作模式转换实例如表2所示。

表2　CTCS-3级列控车载设备的工作模式转换

Table 2　Operation mode conversion of CTCS-3 train control on-board equipment

模式分类	模式转换
SB	SB->SH、SB->FS，SB->OS，SB->CO，
SH	SB->SL，SB->TR，SB->IS
	SH->SB，SH->TR，SH->IS
FS	FS->SB，FS->SH，FS->OS，FS->CO，
	FS->TR，FS->IS
OS	OS->SB，OS->SH，OS->FS，OS->CO，
	OS->TR，OS->IS
CO	CO->SB，CO->SH，CO->FS，CO->OS，
	CO->TR，CO->IS
SL	SL->SB，SL->IS
TR	TR->PT，TR->IS
	PT->SB，PT->SH，PT->FS，PT->OS，
PT	PT->CO，PT->IS
	IS->SB
IS	

CTCS-3级列控系统需求规范的模式转换部分定义了列控车载设备的工作模式、与模式有关的功能以及各模式之间的转换条件[13-14]。主要工作模式对应的车载设备职责：

1）待机模式SB是一种默认模式，司机不能对其进行选择，车载设备启动，自检和测试通过后自动进入待机模式；

2）当车载设备接收到来自RBC的行车许可MA，列车数据和线路数据都具备后，车载设备转入完全监控模式FS，根据动态曲线监控列车运行，并向司机显示列车速度；

3）调车模式SH用于列车进行调车作业时，由司机选择调车，车载设备应向RBC申请授权并在进入调车模式后与RBC断开连接；

4）当地面设备故障，车载设备显示禁止但列车需要继续运行时，由司机选择转入目视行车模式OS，从RBC接收请求，列车每运行一定距离需司机确认一次；

5）引导模式CO用于开放引导信号，接收RBC的请求后司机应在此模式下检查轨道占用；

6）休眠模式SL用于非本务端车载设备，如果开启（异常操作），应转入待机模式SB；

7）当车载设备停用，隔离车载设备的制动功能后，列控车载设备处于隔离模式IS，应向司机指示车载设备已被隔离；

8）当车载设备输出紧急制动命令时进入冒进防护模式TR，应要求司机确认，列车实施紧急制动；

9）冒进后防护模式PT时车载设备应缓解紧急制动，司机选择启动，向RBC发送MA请求。

C3级列控车载设备工作模式转换的CPN模型如图5所示。工作模式的转换是车载安全计算机的主要状态，因此在模型中将工作模式设为库所，模式间转换条件设为替代变迁，用标号pntn表示，p表示模式转换的优先等级，数字越小优先；t表示模式转换条件，在文献[8]《CTCS-3级列控系统需求规范（SRS）》有明确规范。在CPNTools工具的Declarations下定义声明MODE为9种工作模式转换，WRIECOMM设为变量“true”。安全计算机初始工作模式为SB，因此SB的初始标识为1′(6,true)。根据系统需求规范中模式转换条件以及模式转换中车载设备职责，构建模式间转换条件的CPN子页模型，如图6为SB转SH模式的CPN子页模型，

由图 5 可知，SB 转 SH 变迁状态为 p4t6，表示优先级为 4 级，转换条件为 6（司机请求调车模式后，从 RBC 接收到“允许调车”信息）和（列车停车），模型中库所集 P={SB,Driver Shunt Request,RBC Received,On-board Received,SH}，库所集 T={Train Stop Info,Send MSG To RBC,Send Shunt Permission Info,p4_t6}，如图 6 所示。若在工作模式下转换成功，则验证结果显示“true”，否则显示“false”。

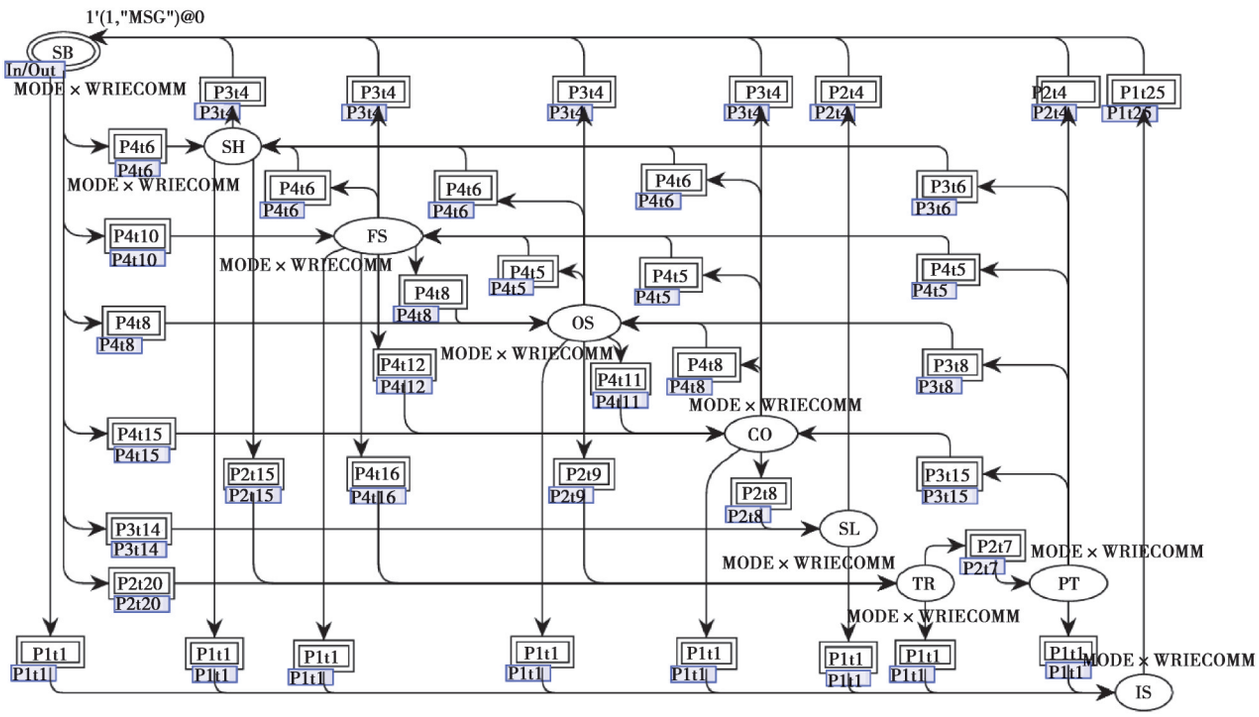

图 5 模式转换的 CPN 模型

Fig. 5 CPN model for pattern transformation

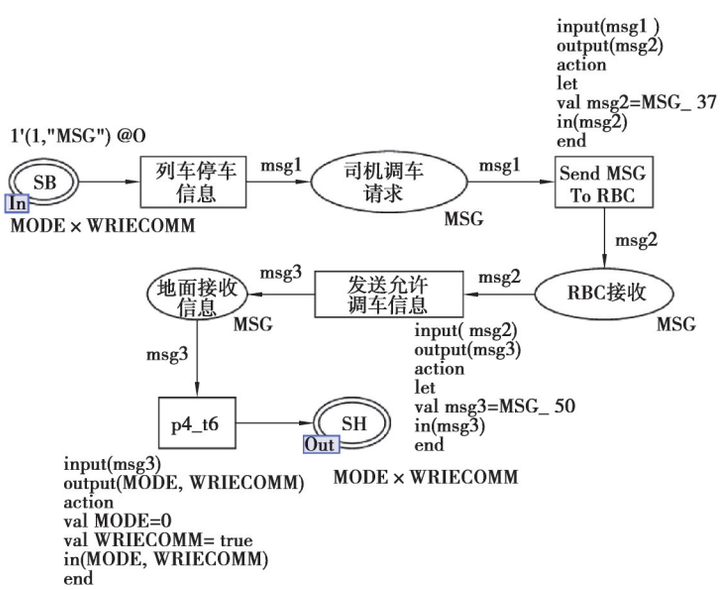

图 6 SB 模式转 SH 模式的 CPN 子页模型

Fig.6 CPN model of SB mode to SH mode

3　CPN模型的验证与分析

3.1　CPN模型的验证

有色Petri网建模语言对模型的验证是用ASK-CTL分支时序逻辑公式描述系统的性质，通过对系统模型进行系统逻辑性的验证分析，例如系统的自循环终端特性、死锁特性等来证明系统模型是否可执行，从而得出构建的CPN模型是否满足系统规范要求的规则以及各组件之间的交互是否符合规范流程。根据对系统需求规范中系统属性分析，对构建的车载设备CPN功能模型以及模式转换CPN模型进行了自循环终端检测、死锁和活锁检测验证。验证结果如下：

对所建车载设备CPN模型进行自循环终端检测是为了验证系统中死标识的合理性，对模型执行ASK-CTL公式，由图7可知验证结果为“There is no loop terminal!”。

```
fun SelfLoop Terminal n=(OutNodes(n)=[n])
fun InvalidTerminal()=PredNodes(EntireGraph,fn n=>(SelfLoop Terminal n),NoLimit);
let
 val fid=TextIO.openOut" verfication results.txt"
 val_=if In ValidTerminal()=[]
 val_=TextIO.output(fid," There is no loop terminal\n" )
in
 TextIO.closeOut(fid)
end;
```

verfication result - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

There is no loop terminal!

图7　车载设备自循环终端验证

Fig. 7　Vehicle equipment self-circulation terminal verification

对车载设备CPN模型进行死锁分析，执行ASK-CTL公式，由图8可知验证结果为“No Deadlock Markings!”。

活锁的检查是根据状态空间报告中OG和SCCG节点和弧的数量相同，即同构的，则系统不存在活锁。部分状态空间报告如图9所示。

```
let
 val fid=TextIO.openOut" DeadMarkings.txt"
 val_=TextIO.output(fid," No Deadlock Markings!\n" )
 val_=EvalNodes(ListDeadMarkings()
                fn n=>INT.output(fid,n))
 val_=TextIO.output(fid,length(ListDeadMarkings()))
in
 TextIO.closeOut(fid)
end
```

verfication result - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

No Deadlock Markings!

图8　模式转换死锁验证

Fig. 8　Deadlock validation of mode trans

采用ASK-CTL公式对模型进行自循环验证和死锁分析等，是为了验证模型的逻辑特性，只有系统死标识合理，无死锁及活锁等特性，模型才是安全可执行的。另外，还可通过CPNTools工具对模型进行功能行为特性的检查：如验证系统的活性、可达性、有界性、转移性和公平性等[15]。例如针对图6系统工作状态下进行模式转换规则验证，车载设备初始工作模式始终为待机SB模式，验证系统是否存在某条路径，使待机模式SB转入调车模式SH，验证执行结果“true”，表示系统模型之间可转移。

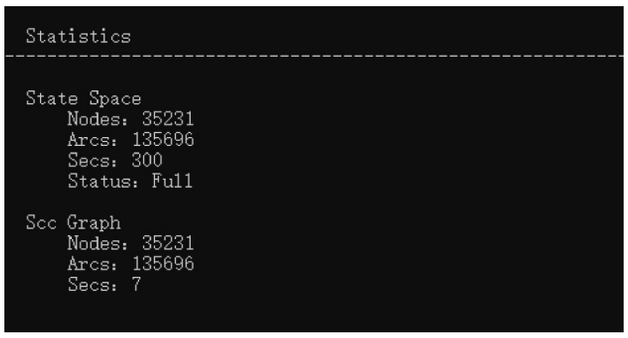

图9 部分状态空间报告

Fig. 9 Part of the state space report

3.2 模型验证结果分析

根据模型验证结果分析系统的属性，只有系统模型中不存在死锁、活锁等属性，才能验证系统功能属性的正确性[16]。

1) 车载设备自循环终端

自循环终端检测是为了验证系统死标识的合理性，由图7的验证结果“There is no loop terminal!”可知CPN模型中不存在自循环终端，验证了系统模型中死标识是合理的，系统模型正确。说明构建的CPN模型满足《CTCS-3级列控系统需求规范（SRS）》要求的车载设备信息交互流程。

2) 模式转换无死锁

无死锁是指系统不会永远停留在一个状态。根据图8ASK-CTL描述的系统性质验证结果“No Deadlock Markings!”，可知系统在模式转换过程中无死锁，系统模型正确。

3) 模式转换无活锁

检查系统活锁的目的是为了发现系统中存在的死循环。由图9可知，“State Space”中节点数和弧与“Scc Graph”中节点数和弧的数量相同，即同构，说明系统中不存在活锁，系统模型正确。

系统模型既无死锁也无活锁，系统功能属性正确，说明构建的CPN模型满足《CTCS-3级列控系统需求规范（SRS）》要求的模式转换功能。

4) 工作状态下系统的行为特性

转移性是指模型中一个模式与另一个模式之间存在迁移关系，即系统可经过转移从一个模式转换到另一个模式，建模验证返回的执行结果为true，表示系统从SB状态可以经过转换步骤迁移到SH状态，由此可知构建的模式转换CPN模型符合系统规范要求的CTCS-3级列控车载设备模式转换条件。

4 结 语

由于CTCS-3级列控车载设备是一个安全苛求性较高的复杂系统，而有色Petri网建模方法能够对模型进行分层建模，适用于复杂系统建模。研究主要分析了列控车载设备功能设计时涉及到的安全问题，对CTCS-3级列控系统车载设备之间的功能信息交互以及车载设备中安全计算机主要状态工作模式转换的各模式之间转换路径和模式之间具体转换流程进行了CPN建模，并在验证工具CPN Tools中使用时序逻辑公式ASK-CTL对所建模型系统功能性质进行描述，根据验证结果分析得到系统功能模型与相关系统需求规范的一致性。此外，提出的有色Petri网建模方法也适用于其他安全性要求较高的复杂系统建模验证研究。该建模验证方法能够对系统进行图形化描述，对复杂系统还可以进行分层建模，大大减少系统空间爆炸的概率。形式化的建模方法能够使建模工具对系统模型进行验证确保系统设计规则的正确性和安全性，减少复杂系统设计规则的不可靠性，对安全苛求性要求较高的复杂系统的设计具有一定的参考意义。

参考文献

[1] 张曙光. CTCS-3级列控系统总体技术方案[M]. 北京: 中国铁道出版社, 2008: 26-37.
Zhang S G. Overall technical scheme of CTCS-3 train control system[M]. Beijing: China Railway Publishing House, 2008: 26-37.(in Chinese)

[2] Hardi Hr, Michael M. Modelling functionality of train control system using petri nets[C]//Fm-rail-bok Workshop. Madrid: DLR, 2013:1-6.

[3] 何文锋. 基于UML的CTCS-3级列控车载设备建模、仿真和测试研究[D]. 北京: 北京交通大学, 2009.
He W F. Research on modeling, simulation and testing of CTCS-3 train control vehicle equipment based on UML[D].Beijing: Beijing Jiaotong University, 2009. (in Chinese)

[4] 曹加云. 基于时间自动机的CTCS-3级列控车载设备建模与验证[D]. 成都: 西南交通大学, 2010.
Cao J Y. Modeling and verification of CTCS-3 train control vehicle equipment based on time automata[D].Chengdu: Southwest Jiaotong University, 2010. (in Chinese)

[5] 牟小玲, 丁晓明, 张望. 基于Petri网的测试用例生成研究进展[J]. 重庆交通大学学报(自然科学版), 2012, 31(1): 163-167.
Mu X L, Ding X M, Zhang W. Research progress in test case generation based on petri nets[J]. Journal of Chongqing Jiaotong University (Natural Science), 2012, 31(1): 163-167.(in Chinese)

[6] 中国铁路总公司. CTCS-3级列车运行控制系统[M]. 北京: 中国铁道出版社, 2013.
China Railway Corporation. CTCS-3 train operation control system [M]. Beijing: China Railway Publishing House, 2013.

[7] Wang R, Zheng W, Liang C, et al. An integrated hazard identification method based on the hierarchical Colored Petri Net[J]. Safety Science, 2016, 88: 166-179.

[8] 铁道部科技司. CTCS-3级列控系统标准规范-CTCS-3级列控系统系统需求规范(SRS)(第一册)[S]. 北京: 中国铁道出版社, 2009.
Department of Science and Technology. Ministry of railways standard specification for CTCS-3 class train control system (SRS) (volume 1) [S]. Beijing: China Railway Publishing House, 2009.(in Chinese)

[9] 马国富, 刘文良, 周建勇, 等. 基于ASK-CTL的有色Petri网模型检验算法研究[J]. 计算机应用与软件, 2015, 32(10): 302-305, 333.
Ma G F, Liu W L, Zhou J Y, et al. Study on coloured petri net model checking based on ask-ctl[J]. Computer Applications and Software, 2015, 32(10): 302-305, 333.(in Chinese)

[10] 赵晓宇, 杨志杰, 吕旌阳. 基于有色Petri网的车载设备模式转换测试序列生成方法[J]. 中国铁道科学, 2017, 38(4): 115-122.
Zhao X Y, Yang Z J, Lv S Y. A Method for generating test sequence of on-board equipment mode conversion based on colored petri nets [J]. China Railway Science, 2017, 38(4): 115-122.(in Chinese)

[11] 胡少强. 基于STPA和有色Petri网的列控系统安全分析[D]. 北京: 北京交通大学, 2018.
Hu S Q. Safety analysis of train control system based on STPA and colored petri net[D].Beijing: Beijing Jiaotong University, 2018. (in Chinese)

[12] Koh K Y, Seong P H. SMV model-based safety analysis of software requirements[J]. Reliability Engineering & System Safety, 2009, 94(2): 320-331.

[13] 赵伟慧. 基于场景的列控车载设备测试用例自动生成方法研究[D]. 北京: 北京交通大学, 2014.
Zhao W H. Research on automatic generation method of test cases for train control vehicle equipment based on scene[D]. Beijing: Beijing Jiaotong University, 2014. (in Chinese)

[14] Lh V, Hong L. Formal development and verification of railway control systems- in the context of ERTMS/ETCS level 2[D]. Copenhagen: DTU, 2015:13-20.

[15] Huang W L, Peleska J. Complete model-based equivalence class testing[J]. International Journal on Software Tools for Technology Transfer, 2016, 18(3): 265-283.

[16] Jensen K, Kristensen L M, Wells L. Coloured Petri Nets and CPN tools for modelling and validation of concurrent systems[J]. International Journal on Software Tools for Technology Transfer, 2007, 9(3/4): 213-254.

(编辑　侯　湘)