文章编号:1671-4598(2017)12-0120-05 DOI:10.16526/j.cnki.11—4762/tp.2017.12.032 中图分类号:TP273 文献标识码:A

应用 ETDFA 生成 CBTC 联锁软件形式化模型的方法

高雪娟[1], 陈启香[2], 郑鸿昌[1]
(1. 株洲中车时代电气股份有限公司 通信信号事业部, 湖南 株洲 412001;
2. 宝鸡文理学院 电子电气工程学院, 陕西 宝鸡 721000)

摘要: CBTC 系统的联锁软件为 SIL4 级的高安全、高可靠软件, 目前广泛使用的软件测试和仿真验证的结果严重依赖选取的测试向量, 要保证高覆盖率的测试十分困难; EN50128 中强烈推荐 SIL4 等级的软件使用形式化方法完成软件需求规格说明书和软件设计, 因此, 采用形式化的方法设计软件, 是构造高可靠、高安全软件的一个重要途径; 总结了现有的 CBTC 系统中联锁子系统集成方式及优缺点, 并使用事件确定有限自动机 ETDFA (event deterministic finite automata) 模型对适用性更优的升级型集成方式的联锁软件的联锁逻辑完成形式化定义, 保证联锁逻辑的正确性, 减少软件的不确定性描述; 以办理进路为例生成联锁对象的 ETDFA 模型, 验证该方法的有效性和可行性; 该方法不仅为 CBTC 联锁软件的设计与开发提供新思路, 而且有助于安全苛求软件的形式化验证与分析, 提高联锁软件的安全性和正确性。

关键词: CBTC; 联锁软件; ETDFA; 形式化方法

Method for Generating CBTC Interlocking Software's Formal System Model Using ETDFA

Gao Xuejuan[1], Chen Qixiang[2], Zheng Hongchang[1]
(1. Signal & Communication Business Unit, Zhuzhou CRRC Times Electric Co., Ltd., Zhuzhou 412001, China;
2. College of Electronics and Electrical Engineering, Baoji Wenli University, Baoji 721000, China)

Abstract: The safety and integrity level of Computer interlocking software in CBTC (communication based train control) system is SIL4, which is high security and high reliability software. The current widely used software testing and simulation results rely heavily on the selected test vector, to ensure high coverage of the test is very difficult. EN50128 strongly recommended SIL4 level of software using formal methods to complete the software requirements specification and software design, therefore, using formal methods to design software is an important way to build high reliability and high security software. This paper summarizes the existing integrated approaches and advantages and disadvantages of the interlocking subsystem in the CBTC system, and uses the ETDFA (event deterministic finite automata) model to realize the formal definition of upgrade type interlocking software, which ensures the correctness of the interlocking logic, and reduces the uncertainty description of the software. This paper takes creating route as an example to generate the ETDFA model of the interlocking object, and verifies the validity and feasibility of the method. This method not only provides new ideas for the design and development of CBTC interlocking software, but also contributes to the formal verification and analysis of security demanding software, and improves the security and correctness of interlocking software.

Keywords: CBTC; interlocking software; ETDFA; formal method

0 引言

CBTC (communication based train control, 基于通信的列车控制) 系统中的联锁软件需支持 CBTC 模式和后备模式下列车的运行防护, 同时能满足混线跑的需求, 因此, 传统的联锁软件并不能满足 CBTC 的更小追踪间隔、更高运输效率的要求。作为安全完整性等级为 SIL4[1] 级的软件, 对 CBTC 联锁软件的安全性、可靠性都有较高的要求。目前对联锁软件安全性的确认, 主要通过模拟验证和仿真测试, 如文献 [2] 研究了计算机联锁软件测试的安全性评价准则, 文献 [3] 通过 EVALPSN 软件模拟验证联锁系统的安全性, 文献 [4] 对联锁系统的 UML 模型用 Rhapsody 模拟分析其安全性。但软件测试和仿真验证的结果严重依赖选取的测试向量, 要保证高覆盖率的测试十分困难。

EN50128[5] 中强烈推荐 SIL4 等级的软件使用形式化方法完成软件需求规格说明书和软件设计。采用形式化的方法设计软件, 是构造高可靠、高安全软件的一个重要途径。统一建模语言 UML (unified modelling language) 的顺序图能描述对象间传递的消息及时间顺序, 但由于 UML 是半形式化语言, 需将系统的顺序图用形式化方法完成描述及验证。

文献 [6-7] 分别基于 B 方法和 Z 语言将 UML 模型进行形式化描述, 但用这两种方法生成的形式化模型对于对详见的交互路径存在表达模糊的问题; 文献 [8] 使用抽象状态机 ASM (abstract state machine) 实现对序列图语义的建模, 但对于复杂的 UML2.0 的序列图, 该方法生成的模型由于缺乏

收稿日期:2017-03-27; **修回日期**:2017-05-27。

作者简介:高雪娟(1990-),女,甘肃白银人,硕士研究生,主要从事城轨信号系统方向的研究。

精确的定义给验证造成了困难；文献［9］以 XYZ/E 的线性时序逻辑为基础完成序列图的形式化描述；文献［10］利用进程代数表达式映射序列图中的交互消息及执行顺序，但缺少直观性；文献［11］使用 Promela 语言描述序列图，但所生成的代码不利于从模型中生成测试用例；文献［12－13］使用 Petri 网对序列图进行形式化描述，但其表达的属性的可判定性依赖其属性[14]；文献［15－19］使用自动机形式化描述序列图，但对序列图中每个对象状态的迁移、对象之间的交互描述的不够清楚。

本文针对序列图中的对象之间的交互，采用基于事件确定有限自动机 ETDFA 描述 UML2.0 序列图，并完成 CBTC 联锁软件的形式化模型生成，验证方法的有效性和可用性。

1　CBTC 联锁软件

1.1 联锁集成方式

目前 CBTC 系统中的联锁集成方式分为兼容型集成方式的联锁和升级型集成方式的联锁[20]，表 1 为两种联锁集成方式的对比。

表 1　不同集成方式的 CBTC 联锁系统对比

	兼容型联锁	升级型联锁
相同点	1. 都具有 CBTC 模式和后备模式； 2. 均与轨旁设备接口，包括计轴、道岔、信号机、站台紧急按钮、站台屏蔽门等。	
核心功能	区域控制器，联锁只作用在后备模式和当 CBTC 模式下的进路中存在道岔时。	联锁
CBTC 进路	实质是移动授权	联锁进路
模式切换	人工切换，CBTC 模式、后备模式以及切换过程中的待机模式	自动切换，只有 CBTC 模式、后备模式
后备模式	双红灯防护的点式 ATP 模式，仅支持列车点式人工 ATP 行车模式	目标距离式的点式 ATP 模式，支持列车点式 ATO 和点式人工 ATP 行车模式。
进路类型	自动解锁进路、人工解锁进路、移动闭塞进路	普通进路、自动通过进路、自动折返进路
引导进路	CBTC 模式下：区域控制器先办理一条人工解锁 CBTC 进路，然后由联锁办理该进路对应的移动闭塞进路；信号开放条件满足后，由区域控制器转发引导信号开放命令。 后备模式：直接由联锁办理	直接由联锁办理
信号显示	CBTC 模式下，采用点灯方式	CBTC 模式下，采用灭灯方式
特点	CBTC 模式下，由于联锁办理进路、解锁进路命令均需区域控制器转发，存在延时，会出现死锁现象；后备模式下，只支持点式人工 ATP。	功能灵活，可用性高，后备模式功能强大，但在 CBTC 模式下采用灭灯方式，不利于硬件设备的故障检测和维修保养。

图 1 为以兼容型方式集成联锁的结构框图，图 2 为以升级型方式集成联锁的结构框图。

本文基于升级型集成方式的联锁实现 CBTC 联锁系统的 ETDFA 模型。

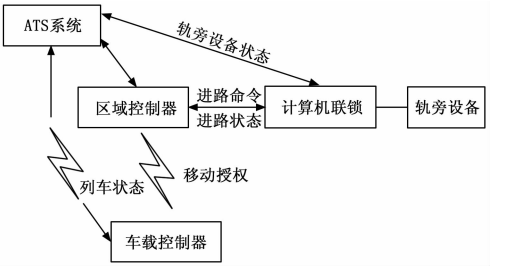

图 1　兼容型集成联锁框图

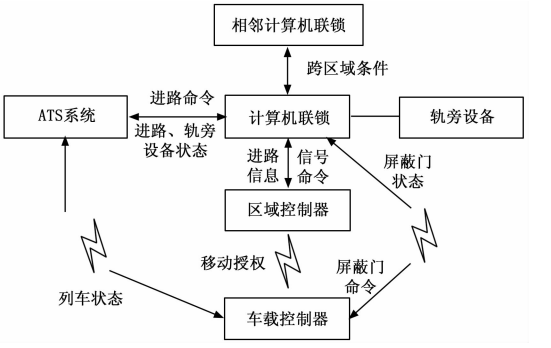

图 2　升级型集成联锁框图

1.2　CBTC 联锁系统功能

图 3 为升级型集成方式的联锁系统结构图。

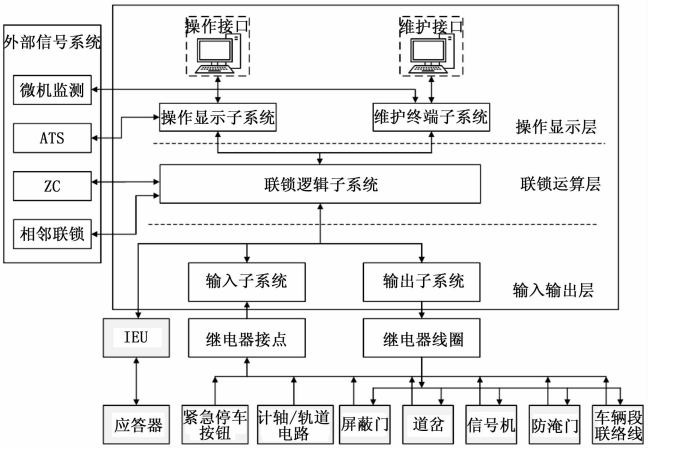

图 3　升级型集成方式联锁系统结构图

CBTC 联锁系统与传统联锁的不同主要有以下几个方面：

1）轨道区段状态：在 CBTC 模式下，由区域控制器向联锁提供列车位置信息；在后备模式下，通过计轴设备获得物理区段占用情况。

2）进路建立：为提高运营效率，缩短追踪间隔，CBTC 系统允许同时有 2 列及以上的列车在信号机所防护的同一条进路中。相比大铁联锁，建立进路时，不再检查进路中区段是否空闲。

3）进路解锁：大铁联锁中进路解锁包括三点检查解锁和取消进路解锁，但在 CBTC 系统下，列车追踪间隔较密，当前行列车还未出清信号机内方区段时，已为后续列车再次办理进

路，后续列车紧随其后驶入该进路，这种情况下，无法通过三点检查实现区段解锁。CBTC 联锁系统针对这种情况有两种解决措施：一是通过 CBTC 系统中列车通过信号机的信息来解锁进路；二是办理进路时，只有当信号机内方第一区段空闲时，才允许办理后续列车的进路[21]。

4）信号显示：CBTC 联锁系统在 CBTC 模式下，若信号机使用传统点灯方式，当信号机发生故障，对运营效率产生极大影响，而且，在 CBTC 模式下，信号开放不检查进路内区段的空闲状态，违背了计算机联锁技术条件中的规定，因此，在 CBTC 模式下，信号显示采用灭灯方式，简化了系统的运用条件。

5）保护进路：类似大铁的延续进路，为避免列车因停车误差而造成安全隐患，CBTC 系统为接车进路设置“保护进路”，一般为进路终端停车点信号机内方一个区段。当接车进路建立、列车驶入触发区段时，“保护进路”自动建立。“保护进路”的解锁方式与大铁延续进路类似。

6）运行方向：与大铁联锁的区间方向电路不同，CBTC 联锁为区间和站内每个区段设置运行方向，随进路的建立而建立，随进路的解锁而清除。

2 UML2.0 序列图

UML2.0 序列图增加了 12 种组合片段[22]，包括 loop，opt，alt，break，par，neg，ref 等，增强了系统对象交互的需求分析与设计中的建模能力。

2.1 序列图的形式化定义

定义 1（序列图）序列图（SD，sequence diagram）通过一个十三元组表示 $SD=(O, E, S, R, M, P, C, OP, F_{em}, F_{eo}, F_{ep}, \rightarrow, <)$，其中，$O$ 是序列图中对象的集合；E 是序列图中事件的集合；S 是发送事件的集合；R 是接收事件的集合，$E=S\cup R$，$S\cap R=?$；M 是消息的集合，每条消息 m（$m\in M$）与该条消息的发送事件 $!\,m$（$!\,m\in S$）和接收事件 $?\,m$（$?\,m\in R$）相关联；P 是组合片段的集合；C 是组合片段执行条件的集合；OP 是操作域的集合，由组合片段各执行条件表示；F_{em} 表示 E 到 M 的函数关系，$F_{em}(e)\in M$；F_{eo} 表示 E 到 O 的函数关系，$F_{eo}(e)\in O$；F_{ep} 表示 E 到 P 的函数关系，$F_{ep}(e)\in P$；$\rightarrow$表示序列图中消息的先后顺序关系；? 表示发送事件与接收事件的二元关系。

2.2 序列图中对象的形式化定义

定义 2（序列图对象）序列图中的对象通过一个六元组表示，$O=(E, P, C, OP, N, F_{ep})$，其中，$N$ 表示事件发生的次序。

图 4 所示为道岔定操命令的序列图及形式化定义，O 联锁

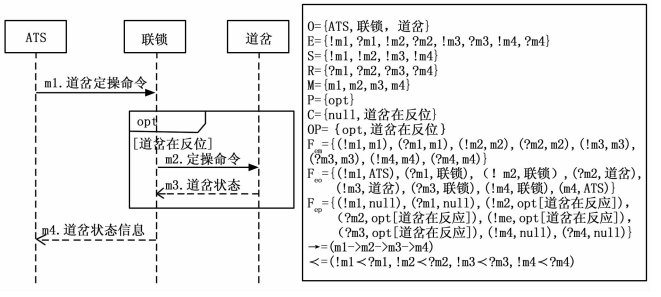

图 4 道岔单操命令的序列图

=（{?m1,!m2,?m3,!m4}，{opt}，{null，道岔在反位}，{opt，道岔在反位}，{1，2，3，4}，{(?m1，null)，(!m2，opt［道岔在反位］)，(?m3，opt［道岔在反位］)，(!m4，null)}），其六元组关系见表 2。

表 2 联锁对象的六元组关系

第一层片段		SD	opt
执行/防护条件			道岔在反位
序号	事件	片段	
1	? m1	●	
2	! m2		●
3	? m3		●
4	! m4	●	

3 序列图形式化模型 ETDFA 生成方法

3.1 事件确定有限自动机 ETDFA

本文使用 ETDFA 的状态迁移描述序列图中的消息交互，实现序列图中事件向对象的映射。状态的一次迁移是指对象发送或接收消息后，从一个状态转移到另一个状态，由事件发生的条件和事件本身构成。序列图中对象的交互过程可通过多个对象的积自动机描述。

定义 3（ETDFA）事件确定有限自动机由一个七元组表示，$M=(S, C_M, E_M, T_{CE}, \delta, s_0, F)$，其中，$S$ 表示状态的集合，$\forall s\in S$；C_M 表示组合片段执行条件的集合；E_M 表示事件集合；T_{CE} 表示状态发生迁移的输入，$T_{CE}=\{(c, e)\mid c\in C_M, e\in E_M\}$；$\delta$ 表示状态迁移函数，$S\times T_{CE}\rightarrow S$；$s_0$ 表示状态机 M 的初始状态，$s_0\in S$；F 表示状态机 M 的终止状态集合，$F\subseteq S$。

3.2 序列图的 ETDFA 模型生成算法

序列图中每个对象的信息交互对应一个事件确定有限自动机 ETDFA，其流程如图 5 所示。

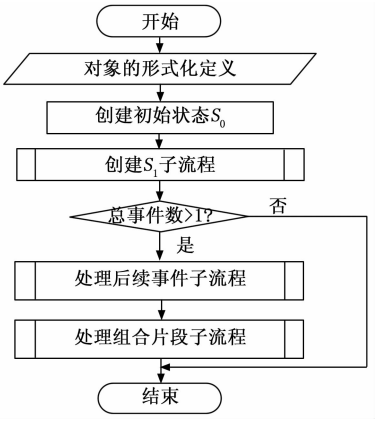

图 5 SD 对象生成 ETDFA 模型流程图

3.2.1 创建 s_1 子流程

创建状态 s_1 的流程如图 6 所示。

3.2.2 处理后续事件子流程

当对象的六元组定义中的 $num>1$ 时，状态 s_i（$i\in 2, \cdots, num$）的创建具体过程分以下几种情况：

（1）若存在以下任一种情况时，$\delta(s_i, s_{i+1})=e_{i+1}$；

①e_i、e_{i+1}均不在组合片段内；

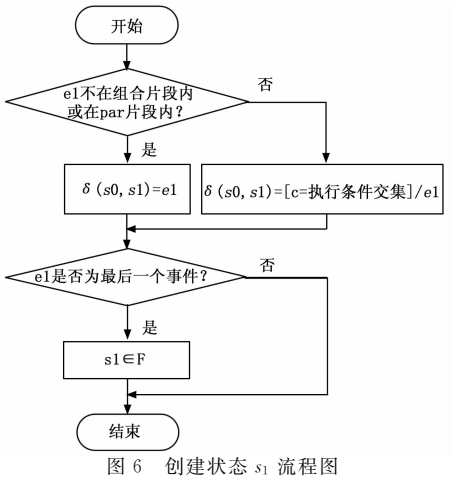

图 6　创建状态 s_1 流程图

②e_i、e_{i+1}在组合片段的相同操作域内；

③e_i 为 par 组合片段内当前操作域的最后一个事件，e_{i+1} 为该组合片段内下一有效操作域内的第 1 个事件；

④e_i 为 alt 或 par 片段内最后一个有效操作域的最后一个事件，e_{i+1}为片段外的第 1 个事件；

⑤e_{i+1}在 par 片段内，e_i 在片段外。

（2）若存在以下任一种情况时，$\delta(s_i, s_{i+1}) = c/e_{i+1}$；

①e_{i+1}在 alt 或 opt 或 loop 或 break 单组合片段内，e_i 在该组合片段外；

②e_{i+1}在多层 alt 的组合片段内，e_i 在该组合片段外。

（3）若存在以下任一种情况时，s_{i+1}为终止状态；

①若 e_{i+1}不在组合片段内，且 e_{i+2}不存在；

②若 e_{i+1}为组合片段内的最后一个事件，且 e_{i+2}不存在；

③若 e_{i+2}在 *alt* 组合片段内，e_{i+1}在组合片段外，且 alt 组合片段操作域的并集不是全集；

④若 e_{i+2}在组合片段内，e_{i+1}在组合片段外，且组合片段后无事件发生；

⑤若 e_{i+1}为 break 组合片段内的最后一个事件，且 break 片段外未嵌套其他片段。

3.2.3　处理组合片段子流程

与组合片段相关的事件生成的状态迁移主要分 7 种情况，见表 3，各种情况的示例图见图 7、图 8。

表 3　组合片段相关的状态迁移

序号	示例图	转移函数	备注
1	图 7（a）	$\delta(si, si+\|N\|+1) = ei+\|N\|+1$	片段为 opt 组合片段或 loop 组合片段或操作域并集非全集的 alt 片段，N 为组合片段内的事件数目。
2	图 7（b）	$\delta(si, sj) = c2/ej$； $\delta(si, sk) = c3/ej$；	组合片段为 alt 或 par，当为 par 片段时，$c=null$
3	图 7（c）	$\delta(sj, si) = ej$； $\delta(sk, si) = ej$；	组合片段为 alt 或 par
4	图 8（a）	$\delta(si, sj) = c/ej$；	
5	图 8（b）	$\delta(si, sj) = ej$； $\delta(si, sk) = ek$；	
6	图 8（c）	$\delta(si, sk) = ek$；	
7	图 8（d）	$\delta(si, sk) = c/ek$；	

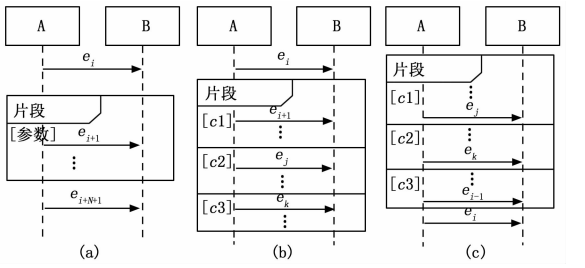

图 7　组合片段示例 1

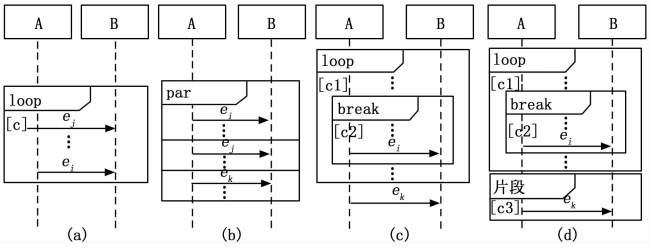

图 8　组合片段示例 2

若序列图中存在 neg 组合片段，在生成对象的自动机时，忽略该片段。

4　CBTC 联锁软件的 ETDFA 模型

4.1　办理进路顺序图

本文以办理进路为例，验证基于 ETDFA 的联锁软件的形式化模型生成方法的实际可行性。

CBTC 系统在 CBTC 模式下办理进路的 UML 顺序图及形式化定义见图 9。

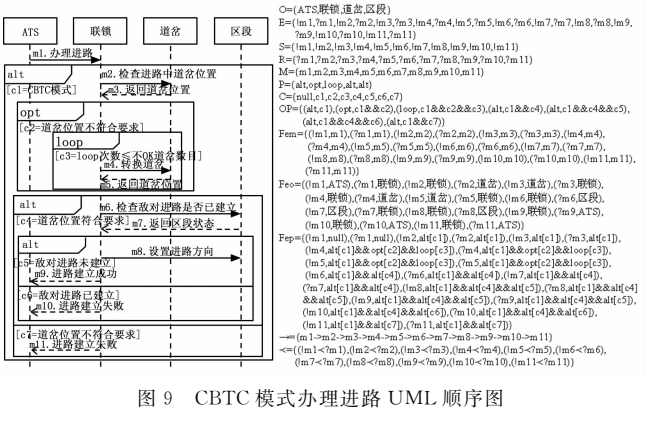

图 9　CBTC 模式办理进路 UML 顺序图

$O_{联锁}$ = ({! m2, ? m3, ! m4, ? m5, ! m6, ? m7, ! m8, ! m9, ! m10, ! m11}, {alt, opt, loop, alt, alt}, {null, c1, c2, c3, c4, c5, c6, c7}, {(alt, c1), (opt, c1&&c2), (loop, c1&&c2&&c3), (alt, c1&&c4), (alt, c1&&c4&&c5), (alt, c1&&c4&&c6), (alt, c1&&c7)}, {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}, {(? m1, null), (! m2, alt[c1]), (? m3, alt[c1]), (! m4, alt[c1]&&opt[c2]&&loop[c3]), (? m5, alt[c1]&&opt[c2]&&loop[c3]), (! m6, alt[c1]&&alt[c4]), (? m7, alt[c1]&&alt[c4]), (! m8, alt[c1]&&alt[c4]&&alt[c5]), (! m9, alt[c1]&&alt[c4]&&alt[c5]), (! m10, alt[c1]&&alt[c4]&&alt[c6]), (! m11, alt[c1]&&alt[c7])})，表 4 为联锁对象

的六元组关系。

表 4 联锁对象的六元组关系

第一层片段		SD	alt						
执行/防护条件			c1						
第二层片段				opt		alt			
执行/防护条件				c1&&c2		c1			
&&c4				c1&&c7					
第三层片段					loop		alt		
执行/防护条件					c1&&c2 &&c3		c1&&c4 &&c5	c1&&c4 &&c6	
序号	事件								
1	? m1	●							
2	! m2		●						
3	? m3		●						
4	! m4				●				
5	? m5				●				
6	! m6					●			
7	? m7					●			
8	! m8						●		
9	! m9						●		
10	! m10							●	
11	! m11								●

4.2 联锁对象的 ETDFA 模型

使用第 4 节描述的 ETDFA 模型生成方法，CBTC 联锁对象的 ETDFA 的创建过程为：

1）设置初始状态 s_0；

2）输入状态迁移字母表：

$T_{CE}=\{(c,e)|c\in C_M,e\in E_M\}$；

$C_M=\{$(alt, c1), (opt, c1&&c2), (loop, c1&&c2&&c3), (alt, c1&&c4), (alt, c1&&c4&&c5), (alt, c1&&c4&&c6), (alt, c1&&c7)$\}$；

$E_M=\{$! m2, ? m3, ! m4, ? m5, ! m6, ? m7, ! m8, ! m9, ! m10, ! m11$\}$

3）根据算法依次创建状态 s_1，s_2，…，s_{11}，状态 s_9、s_{10}、s_{11}属于终止状态；

4）组合片段处理生成的状态迁移。

生成的联锁对象的自动机的七元组定义为：

M 联锁$=(\{s_0,s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8,s_9,s_{10},s_{11}\},\{C_M\},\{E_M\},\{C_M\times E_M\},\{\delta(s_0,?\ m1)=s_1,$

$\delta(s_1,[c1]/!\ m2=s_2)$,

$\delta(s_2,[c1]/?\ m3)=s_3$,

$\delta(s_3,[c1\&\&c2\&\&c3]/!\ m4)=s_4$,

$\delta(s_4,[c1\&\&c2\&\&c3]/?\ m5)=s_5\}$,

$\delta(s_5,[c1\&\&c4]/!\ m6)=s_6$,

$\delta(s_3,[c1\&\&c4]/!\ m6)=s_6$,

$\delta(s_6,[c1\&\&c4]/?\ m7)=s_7$,

$\delta(s_7,[c1\&\&c4\&\&c5]/!\ m8)=s_8$,

$\delta(s_8,[c1\&\&c4\&\&c5]/!\ m9)=s_9$,

$\delta(s_5,[c1\&\&c4\&\&c6]/!\ m10=s_{10}$,

$\delta(s_5,[c1\&\&c7]/!\ m11)=s_{11}$,

$\delta(s_3,[c1\&\&c4\&\&c6]/!\ m10=s_{10}$,

$\delta(s_3,[c1\&\&c7]/!\ m11)=s_{11}\},\{s_0\},\{s_9,s_{10},s_{11}\})$

图 10 为联锁对象的 ETDAF 模型。

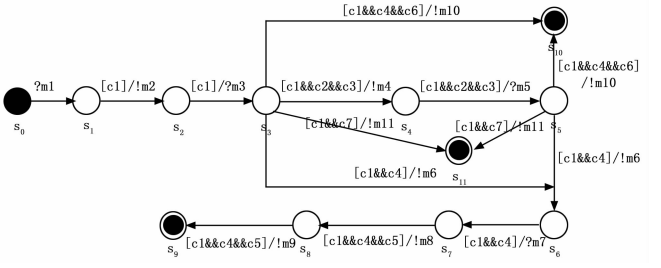

图 10 联锁对象 ETDFA 模型

5 结论

本文采用 UML 顺序图描述 CBTC 联锁系统的联锁逻辑，从顺序图中提取单个对象的相关信息，通过形式化模型生成方法获得单个对象的 ETDFA 模型。本方法不仅为 CBTC 联锁软件的设计与开发提供新思路，而且有助于安全苛求软件的形式化验证与分析，提高联锁软件的安全性和正确性。

参考文献：

[1] 中华人民共和国铁道部. TB/T 3027－2015 计算机连锁技术条件 [S]. 北京：中国铁道出版社，2015.

[2] 吴芳美. 计算机联锁软件基于测试的安全性评价基准研究 [J]，铁道学报，2005，27 (3)：97－101.

[3] Nakamatsu K，Kiuchi Y，Chen W Y，et al. Intelligent railway interlocking safety verification based on annotated logic program and its simulator [A]. 2004 IEEE International Conference on Networking，Sensing and Control [C]. IEEE，2004，1：694－699.

[4] Hon Y M，Kollmann M. Simulation and verification of UML－based railway interlocking designs [A]. Automatic Verification of Critical Systems [C]. 2006：168－172.

[5] CENELEC. EN50128－2011 Railway applications－Communication，signaling and processing systems－Software for railway control and protection systems [S]. Brussels：CENELEC，2011.

[6] Ben Ammar B，Bhiri M T，Souquières J. Incremental development of UML specifications using operation refinements [J]. Innovations in Systems and Software Engineering，2008，4 (3)：259－266.

[7] 李景峰，陈 平. 基于 Z 规范的统一建模语言序列图语义分析方法 [J]. 西安电子科技大学学报（自然科学版），2003，30 (4)：519－524.

[8] Zhou X，Shao Z. ASM Semantic Modeling and Checking for Sequence Diagram [A]. ICNC [C]. 2009 (5)：527－530.

[9] Gan J，Zhang S，Wen B. Research of modeling method based on UML2. 0 and temporal logic [A]. 2009 1st International Conference on Information Science and Engineering (ICISE) [C]. IEEE，2009：5033－5036.

[10] Tribastone M，Gilmore S. Automatic translation of UML sequence diagrams into PEPA models [A]. QEST'08. Fifth International Conference on Quantitative Evaluation of Systems，2008 [C]. IEEE，2008：205－214.

[11] Lima V，Talhi C，Mouheb D，et al. Formal verification and validation of UML 2. 0 sequence diagrams using source and destination of messages [J]. Electronic Notes in Theoretical Computer Science，2009，254：143－160.

(下转第 136 页)

作和查看结果；标签、编辑框、按钮等整齐清楚；多个测试功能按模块分页面显示；界面上有必要的操作监控和文件路径；保存、解析、显示收到的数据可关联设置，可对测试数据进行管理，比对分析等[12]。

经过总结，工作界面上应包括：

1）模拟数据源发送，模拟多路工程遥测数据发送，数据以文本文件或二进制文件的形式输入，也可以在界面上手动编辑并输入；

2）遥控指令发送，可通过界面新增、修改或删除指令，可选择不同的发送模式，如单次发送、周期发送或组合发送；

3）模拟量遥测参数接收，遥测参数实时显示，曲线监控界面可配置，测试数据自动保存到文件，可以事后回放；

4）遥控数据接收，设置存储路径，可保存数据，实时或事后数据比对，计算帧计数并做连续性判读、统计错误消息和误码率等信息；

5）数字量遥测数据接收，数据解析并实时显示，存储路径界面可设置，可保存数据。把接收到的数据按照解析定义按位解析，显示成特定含义或控制指示灯的亮与灭。遥测解析实时或事后可选择，测试数据本地存盘。

3.4 软件测试

本软件已在多个卫星型号上应用实践。现摘取其中两个型号单机的应用实例进行软件测试，某型号功放级地面测试软件实例如图 5 所示，某型号 Ka 应答机地面测试软件实例如图 6 所示。测试结果表明，该软件功能完善，性能稳定，界面友好，能够实现不同的测试方案，具有一定的通用性和扩展性，满足了地面测试的各项需求。

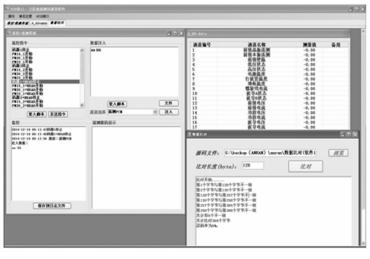

图 5 卫星地面测试软件实例 1

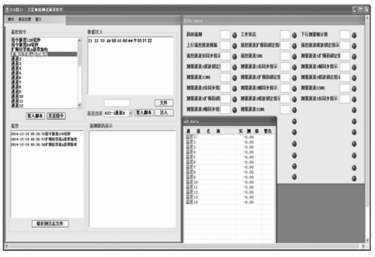

图 6 卫星地面测试软件实例 2

4 结束语

本文设计的 USB 通用化地面测试软件，与以往的专用软件相比，其通用化的设计可以满足当前研制任务周期短、密度大、技术更新快的需求，是一个节省研制成本，确保测试任务高效完成的重大创新。本软件能够满足卫星数传分系统和测控分系统大部分单机地面测试的需求，并已在多个型号上得到验证。

参考文献：

[1] 马 骏. 通用虚拟测试系统设计方法研究 [D]. 西安：西北工业大学，2006.

[2] 程 诗. 基于高频信号的无线电设备自动测试系统的研究与实现 [D]. 广州：华南理工大学，2013.

[3] 刘宇宏，陈 龙，王亚鸣. 基于北斗的连续运行卫星定位综合服务平台设计及其应用 [J]. 上海航天，2014，31 (1)：37－43.

[4] 刘 雪，陈宇峰. 三余度电液伺服阀静态特性测试系统研制 [J]. 上海航天，2014，31 (4)：64－68.

[5] 范 群. 产品通用化测试系统研究与实现 [J]. 计算机与数字工程，2008，36 (8)：54－57.

[6] 徐 明，王金龙. 分离模块化航天器系统评估和优化设计研究 [J]. 上海航天，2015，32 (6)：8－16.

[7] 范凤军，杨 正，祁士青. 基于 LabVIEW 的星用铷频标多通道时差数据自动采集系统 [J]. 上海航天，2015，32 (5)：69－72.

[8] 云 颖，宋雷军. 基于 CAN 总线的星载软件测试系统设计 [J]. 上海航天，2014，31 (5)：65－68.

[9] 蔚保国，李 隽，易卿武. 卫星地面站通用化自动测试系统的研究与实现 [J]. 现代防御技术，2006，34 (5)：28－33.

[10] 刘 军，邹 文，张奎华，等. 基于 CAN 总线的振动试验智能监控系统软件设计 [J]. 计算机测量与控制，2016，24 (6)：136－138.

[11] 王立胜，魏 然，沈宗月，等. 空间站信息系统仿真验证平台设计 [J]. 上海航天，2014，31 (1)：63－68.

[12] 姚洪奎. 数字示波器自动化测试软件系统设计与实现 [D]. 成都：电子科技大学，2010.

(上接第 124 页)

[12] Li G, Yao S. Research on mapping algorithm of UML sequence diagrams to object Petri nets [A]. GCIS'09. WRI Global Congress on Intelligent Systems, 2009 [C]. IEEE, 2009, 4: 285－289.

[13] Nematzadeh H, Deris S B, Maleki H, et al. Evaluating reliability of system sequence diagram using fuzzy Petri net [J]. Int' l Journal of Recent Trends in Enginnering, 2009, 1 (1): 142－147.

[14] Esparza J. Decidability and complexity of Petri net problems—an introduction [Z]. Lectures on Petri Nets I: Basic Models. Springer Berlin Heidelberg, 1998: 374－428.

[15] Knapp A, Wuttke J. Model checking of UML 2. 0 interactions [A]. International Conference on Model Driven Engineering Languages and Systems [C]. Springer Berlin Heidelberg, 2006: 42－51.

[16] Harel D, Kleinbort A, Maoz S. S2A: A compiler for multi－modal UML sequence diagrams [A]. International Conference on Fundamental Approaches to Software Engineering [C]. Springer Berlin Heidelberg, 2007: 121－124.

[17] Harel D, Maoz S. Assert and negate revisited: Modal semantics for UML sequence diagrams [J]. Software & Systems Modeling, 2008, 7 (2): 237－252.

[18] Broy M, Jonsson B, Katoen J P, et al. Model－Based testing of reactive systems [M]. Berlin: Heidelberg Springer－Verlag, 2005: 615－616.

[19] Lynch N A, Tuttle M R. An introduction to input/output automata [J]. CWI Quarterly, 1988, 2 (3): 219－246.

[20] 赵晓峰. 计算机联锁在 CBTC 系统中的两种集成方式 [J]. 铁道通信信号，2012，48 (11)：26－29.

[21] 凌祝军. CBTC 系统中的联锁技术研究 [J]. 铁道通信信号，2009，45 (9)：12－14.

[22] Jim Arlow, Ila Neustadt. UML 2.0 和统一过程 [M]. 方贵宾，胡辉良，译. 第二版. 北京：机械工业出版社，2006.