# 基于混成自动机的CPS行为建模与属性验证

拓明福[1,2]， 周兴社[1]， 李嘉林[2]， 李 辉[2]
(1.西北工业大学计算机学院，西安，710129；2.空军工程大学理学院，西安，710051)

**摘要** 系统实时性、安全性和可靠性等非功能属性是信息物理系统在诸多领域应用的关键因素。论文在分析CPS模型构建与分析验证中面临的挑战的基础上，提出了一种CPS行为建模与属性验证方法。该方法首先基于混成自动机对CPS的行为进行建模，然后将此模型转换为混合程序模型，最后在定理证明器KeYmaera中对HP模型的属性进行形式化验证。文中论述了行为模型描述语言的结构，建立了混成自动机模型与HP模型之间的转换规则，分析了模型转换的一致性。应用实例表明：该方法既能简单直观地描述CPS动态行为，又能对CPS的属性进行严格的形式化验证，且有效避免了形式化验证中的状态空间爆炸问题。

**关键词** 信息物理系统；模型验证；混成自动机；混合程序；模型转换
**DOI** 10.3969/j.issn.1009-3516.2016.03.008
**中图分类号** TP393 **文献标志码** A **文章编号** 1009-3516(2016)03-0040-05

# Behavior Modeling and Attribute Validation of Cyber-Physical System (CPS) Based on Hybrid Automata

TUO Mingfu[1,2], ZHOU Xingshe[1], LI Jialin[2], LI Hui[2]
(1.School of Computer, Northwestern Polytechnical University, Xi'an 710072, China;
2. Science College, Air Force Engineering University, Xi'an 710051, China)

**Abstract**: Non-function attribute such as real-time, security, and reliability, etc. is a key factor in cyber-physical systems applied to many areas. On the basis of analyzing CPS modeling and verification, a CPS behavior modeling and attribute verification is proposed in this paper. In this method, three steps are as follows: (1) to model the behavior of CPS based on hybrid automata; (2) to convert this model to HP model; (3) to verify the HP model in KeYmarera. The structure of behavior model language is introduced. Rules of converting hybrid automata model to hybrid program (HP) model are established. The consistency of the conversion is analyzed. The result shows that this method can depict the behavior of CPS simply and intuitively, and can also verify the properties of CPS strictly. By doing so, this avoids state space explosion in formal verification effectively.

**Key words**: cyber-physical system (CPS); model verification; hybrid automata; hybrid program (HP); model conversion

**收稿日期**：2015-12-11
**基金项目**：国家自然科学基金(61472443)
**作者简介**：拓明福(1979—)，男，宁夏中卫人，讲师，博士生，主要从事分布式计算，CPS分析与验证研究.E-mail: mftuo@163.com

*引用格式：拓明福，周兴社，李嘉林，等. 基于混成自动机的CPS行为建模与属性验证[J]. 空军工程大学学报：自然科学版，2016，17(3)：40-44. TUO Mingfu, ZHOU Xingshe, LI Jialin, et al. Behavior Modeling and Attribute Validation of Cyber-Physical System (CPS) Based on Hybrid Automata[J]. Journal of Air Force Engineering University: Natural Science Edition, 2016, 17(3): 40-44.*

信息物理系统(Cyber-Physical Systems，CPS)的实时性、安全性和可靠性等特性往往是其在关键领域应用的前提。CPS 分析和验证技术可以在系统设计阶段确定 CPS 是否满足实际应用需求，在提高和保障系统安全性、可靠性和实时性等方面起到了关键作用[1-2]。然而，CPS 系统中通常存在的大规模复杂异构性、通信不确定性以及计算过程同步或异步管理需求等情况，这些因素使 CPS 的属性验证比传统的嵌入式系统的属性验证更加复杂[3-5]。因此，研究面向 CPS 的属性分析与验证技术具有重要意义。

# 1　CPS 属性分析与验证

## 1.1　CPS 属性分析与验证技术

随着 CPS 应用越来越广泛，关于 CPS 分析与验证技术的研究也不断深入。对经典的属性分析验证算法进行优化和扩展是 CPS 属性分析与验证的技术途径之一。如从实时操作系统、实时网络传输协议等方面研究 CPS 实时性；利用故障树、Markov 链等手段研究 CPS 的可靠性[6]。也有研究者使用着色 Petri 网(Colored Petri Nets，CPNs)对实时并发系统进行建模，借助 CPN 工具对 CPS 的实时性、安全性进行分析和仿真[7-8]。这些技术对 CPS 计算实体的分析和验证比较成熟，但针对交互实体和物理实体的分析与验证相对薄弱。

近年来，模型检验和定理证明等形式化方法越来越多地被应用于 CPS 分析验证中[9-12]。模型检验的主要优点是自动化程度高，但由于复杂的混成系统的模型检验问题都是不可判定的，此类方法能够处理的连续变量的数量很小，达不到工业应用的要求。从实际应用角度看，定理证明的思路更适合于复杂 CPS 的属性分析与验证[13-14]。其中，Platzer 提出的微分动态逻辑(Differential Dynamic Logic，dL)，语法严谨、语义清晰，在安全相关系统的分析验证中应用较为广泛。其操作模型为混合程序(Hybrid Programs，HP)[15-17]。

## 1.2　CPS 建模与属性验证工具

对 CPS 进行建模是对其属性进行分析验证的前提。在系统建模阶段，为了使模型直观易懂，通常采用通用 CPS 建模工具。为便于形式化验证，又需要将通用模型转换为形式化模型。

CPS-ADL 是用于 CPS 建模、分析与仿真的综合集成软件平台。该平台根据 CPS 的建模、分析和仿真需求对 AADL 进行了扩展，如增加了用于描述系统中物理单元和交互单元的构件等。本文在该平台上扩展了 CPS 行为建模功能[18-19]。

KeYmaera 是一种自动化程度较高的定理证明工具，支持微分动态逻辑，适合于复杂混成系统的分析。KeYmaera 已被成功用于空中交通管制、高速列车系统和汽车自动巡航控制系统中，以减少潜在的危险隐患。

# 2　基于混成自动机的 CPS 行为建模与属性验证

## 2.1　行为建模与属性验证框架

在 CPS-ADL 中基于混成自动机对 CPS 进行行为建模，并将该行为模型转换为 HP 模型。然后将与属性相关的约束条件和由 CPS 模型转换得到的 HP 模型作为定理证明工具 KeYmaera 的输入，进行属性推理验证。图 1 给出了 CPS 行为建模与属性验证框架。

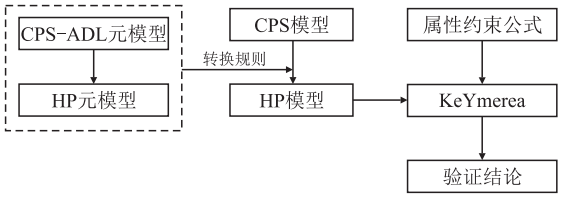


图 1　CPS 行为建模与属性验证框架

Fig.1　The framework for modeling and verification of CPS behavior

在该框架下，将 CPS 属性验证分为 3 个步骤：首先在满足模型转换一致性的前提下建立 CPS-ADL 元模型与 HP 元模型之间的转换规则；然后按照这些转换规则将 CPS-ADL 中建立的具体应用模型转化为对应的 HP；最后将需要验证的属性描述为符合 dL 的属性约束公式，将该属性约束公式和前面转换得到的 HP 模型一起输入 KeYmarea 验证系统能否满足属性约束。

## 2.2　CPS 行为建模

CPS 的模型一般分为静态结构模型和动态行为模型 2 个方面。结构模型描述了系统各组件之间的联系，行为模型描述了系统的运行机制，是影响 CPS 属性的重要因素，也是本文讨论的重点。离散的计算过程和连续的物理过程深度融合是 CPS 的最典型的特征。针对这一特征，本文基于混成自动机对 CPS 行为建模。

描述混成自动机的程序代码主要由 2 部分组成：第 1 部分为 INTERFACE，即声明系统中所有的变量和参数，包括 STATE，INPUT，OUTPUT 和 PARAMETER 4 个函数，分别表示系统的状态、

输入、输出和参数列表,并接受编译器规则类型的检测;第 2 部分为 IMPLEMENTATION,由各个定义变量间关系的专用函数构成,每个函数由系统设计人员根据实际系统运行情况来刻画。一个 CPS 系统的声明如下:

```
SYSTEM name {
INTERFACE {
}
IMPLEMENTATION{
}
}
```

系统的实现部分的函数,即 IMPLEMENTATION 中的主要的关系定义专用函数,包括 AUX、AD、DA、LOGIC、CONTINUOUS、LINEAR 以及 AUTOMATA 等函数。

### 2.3 模型转换的一致性

将 CPS 的行为模型转换为 HP 模型必须保证二者的语义一致性。这要求用于描述 2 种模型的语言 $L_1$ 和 $L_2$ 应该满足如下约束:$L_1$ 和 $L_2$ 在语义上对等,即 $L_1$ 的概念集在 $L_2$ 中具有语义对等的概念集,反之亦然。描述行为模型的语言中包含描述系统运行机制部分和用于图形化显示的部分,模型转换时只需要转换描述系统运行机制部分。

### 2.4 模型转换规则

在保证模型转换语义一致性的前提下,建立从 CPS-ADL 元模型到 HP 元模型之间的转换规则。这里给出一些主要的转换规则。

数据转换规则:将 INTERFACE 部分的 INPUT 函数、OUTPUT 函数、PARAMETER 函数和 IMPLEMENTATION 部分的 AUX 函数转换为 HP 模型中的数据定义部分。

状态转换规则:将 STATE 函数中的每个状态变量转换为 HP 模型中的一个 Mode(对应一段混合子程序)。

迁移转换规则:将 IMPLEMENTATION 部分的 CONTINUOUS 函数中各状态变量的动态变化公式分别转换为 HP 模型中相应 Mode 的动力学过程描述部分。将 AD 函数、DA 函数和 LOGIC 函数转换为 HP 模型中相应 Mode 的条件语句部分。

约束转换规则:MUST 函数转换为 HP 模型中的初始条件部分。

## 3 应用实例

欧洲列车控制系统(European Train Control System,ETCS)是一个典型的 CPS 应用,见图 2。系统主要由列车 train 和无线闭塞控制器 RBC 2 个单元组成。列车只允许在 RBC 为其授权的移动范围(Movement Authority,MA)内运行,RPC 根据其管辖范围内列车运行情况动态计算 MA,并向列车发送。列车控制机构按照 MA 对列车运动进行调整,保证列车始终处于 MA 内。系统的控制目标是在确保运行安全的前提下尽可能提高道路上列车的吞吐率。

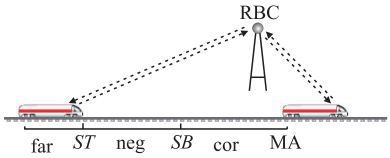


图 2 ETCS 的运行机制

Fig.2 The operation mechanism of ETCS

按照列车的位置不同,可以把列车的运行过程分为 far、neg 和 cor 3 个阶段。far 表示列车距离 MA 的右边界较远,此时可以任意调整列车的速度;neg 为协商阶段,列车可能收到来自 RBC 的新的 MA,将授权位移向右不断延伸;若列车没有及时收到新 MA,则列车开始刹车,转入 cor 阶段,调整列车运行速度,当列车收到来自 RBC 的紧急事件消息 emergency 时,也转入 cor 阶段。图中 $ST$ 表示开始协商的时刻,$SB$ 表示开始刹车的时刻。

为了便于下文描述,我们假设以下变量:$m$ 表示当前 MA 值;$A$ 表示列车的最大加速度;$B$ 分别表示列车的最大减速度;$p$ 表示列车在当前 MA 的位置;$v$ 表示列车的当前速度;$t$ 是自动列车保护单元动态确定的安全运行时间;$T$ 表示列车最长可以运行的时间,超过此时间需要重新调整列车行驶速度;msg 表示行驶过程中是否有紧急情况发生,如果有,则列车减速;$rv$ 表示在当前 MA 内的推荐速度,超过该速度则应该减速。根据物理学原理,可以计算出 $SB$ 的最小值,见式(1):

$$SB \geqslant \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}T^2 + Tv\right) \qquad (1)$$

在 CPS-ADL 平台中,描述 ETCS 行为模型的程序代码如下:

```
SYSTEM  ETCS {
INTERFACE {
    STATE {REAL v ;
           REAL a;
           REAL p;}
    INPUT {REAL rv ;
           REAL m ;
           BOOL msg;}
    OUTPUT { BOOL in MA; }
```

```
    PARAMETER {
        REAL A=2, B=1, T=5,v0=0;
}
}
IMPLEMENTATION {
    AUX {REAL t;
         REAL a1 [-B,0];
         REAL a2 [-B,A];
    BOOL fast,slow,atsb;
    BOOL emergency; }
    AD  {fast = v>=rv;
         slow = v<=rv;
         atsb = (m-p)<=SB;
msg= emergency ;}
    DA  {a = {IF fast THEN a1}
         a = {IF slow THEN a2}
         a={IF atsb | emergency THEN
         -B };
    }
    CONTINUOUS {v=v0+a*t;
    p=v0*t+1/2*a*t^2;}
    OUTPUT {inMA ={IF p<m THEN true
                   ELSE false}
        }
    }
}
```

按照元模型间的转换规则，上述行为模型转换得到的 HP 模型如下：

$$\begin{aligned}
&\mathrm{ETCS} \equiv (\mathrm{rpc} \cup \mathrm{train})^*\\
&\mathrm{rpc} \equiv (\mathrm{m}=*;\ \mathrm{rv}=*;\ ?\ (\mathrm{rv}>0)) \cup\ \mathrm{msg}:=\mathrm{emergency}\\
&\mathrm{train} \equiv \mathrm{lspd};\ \mathrm{hspd};\ \mathrm{atp};\ \mathrm{drive}\\
&\mathrm{lspd} \equiv\ ?\ (\mathrm{v} \leqq \mathrm{rv});\ \mathrm{a}:=*;\ ?\ (-\mathrm{B} \leqq \mathrm{a} \leqq \mathrm{A});\\
&\mathrm{hspd} \equiv\ ?\ (\mathrm{v} \geqq \mathrm{rv});\ \mathrm{a}:=*;\ ?\ (-\mathrm{B} \leqq \mathrm{a} \leqq 0);\\
&\mathrm{atp} \equiv \mathrm{SB}:=\frac{\mathrm{v}^2}{2\mathrm{B}}+1)(\frac{\mathrm{A}}{\mathrm{B}}+1)(\frac{\mathrm{A}}{2}\mathrm{T}^2+\mathrm{T}*\mathrm{v});\\
&\quad \mathrm{if}(\mathrm{m}-\mathrm{p} \leqq \mathrm{SB} \vee \mathrm{msg}=\mathrm{emergency})\\
&\quad \mathrm{a}:=-\mathrm{B}\\
&\quad \mathrm{fi}\\
&\mathrm{drive} \equiv\ \mathrm{t}:=0;\ (\mathrm{p}'=\mathrm{v};\ \mathrm{v}'=\mathrm{a};\\
&\quad \mathrm{t}'=1 \wedge \mathrm{v} \geqq 0 \wedge \mathrm{t} \leqq \mathrm{T});
\end{aligned}$$

利用 dL 公式 $\omega \rightarrow [\mathrm{ETCS}^*]\Phi$ 进行系统属性规约。其中，$\omega$ 为初始条件，$\Phi$ 为需要验证的结论：

$$\omega \equiv A \geqslant 0 \wedge B \geqslant 0 \wedge 2B(m-p) \geqslant v^2$$

$$\Phi \equiv p \leqslant m$$

在 KeYmaera 中进行验证，得到在满足初始条件 $\omega$ 下上述 dL 公式成立，从而证实了待验证结论成立。

从实验结果来看，此验证方法有效避免了模型检测等形式化验证方法存在的状态空间爆炸问题，并且验证步骤比采用 PHaver 等形式化验证工具少，与故障树、Markov 链等传统的属性分析与验证方法相比，能更好地分析验证 CPS 中物理实体的连续变化过程以及物理实体与计算实体的交互。

## 4　总结与展望

使用通用的可视化建模工具对 CPS 建模，然后将模型转换为形式化模型进行验证，这是 CPS 属性分析与验证的有效途径之一。这种方法不仅可以使 CPS 模型直观、易懂，而且便于对模型进行形式化验证。

下一步我们将继续研究混成自动机描述语言的层次化问题，并进一步完善 CPS-ADL 元模型和 HP 元模型的转换规则，提高转换的自动化程度。

**参考文献(References)：**


[1] 梁晓龙，张佳强，祝捷，等.基于 CPS 的空中交通系统架构及能力涌现方法[J].空军工程大学学报：自然科学版，2016，17(1)：1-7.
LIANG Xiaolong，ZHANG Jiaqiang，ZHU Jie，et al. Air Traffic Control System Architecture and Ability Emergence Method Based on Cyber Physical System [J]. Journal of Air Force Engineering University：Natural Science Edition，2016，17(1)：1-7.(in Chinese)

[2] 朱智，雷永林，朱宁，等. 面向网络化防空反导体系的可组合建模框架[J].国防科技大学学报，2014，36(5)：189-193.
ZHU Zhi，LEI Yonglin，ZHU Ning，et al. Composable Modeling Frameworks for Networked Air Missile Defense System[J].Journal of National University of Defense Technology，2014，36(5)：189-193.(in Chinese)

[3] LEE E. CPS Foundations[C]//Proceedings of the 47th ACM/IEEE Design Automation Conference. Washington DC：IEEE Computer Society，2010：737-742.

[4] BAHETI R，GILL H.Cyber-Physical Systems[J].Impact of Control Technology，2011，13(4)：1-6.

[5] 景博，周伟，黄以锋，等.信息物理融合系统及其应用[J].空军工程大学学报：自然科学版，2014，15(2)：1-6.

JING Bo, ZHOU Wei, HUANG Yifeng, et al. Research of Cyber-Physical Systems and It's Applications[J]. Journal of Air Force Engineering University: Natural Science Edition, 2014,15(2):1-6.(in Chinese)

[6] LEONARDI F, PINTO A, CARLONI L P. Synthesis of Distributed Execution Platforms for Cyber-Physical Systems with Applications to High-Performance Buildings[C] //Proceedings of the IEEE/ACM International Conference on Cyber-Physical Systems. Chicago, USA: IEEE, 2011:215-224.

[7] JHA Susmit, GULWANI Sumit, SESHIA A Sanjit, et al. Synthesizing Switching Logic for Safety and Dwell-Time Requirements[C]//Proceeding of the 1st ACM/IEEE International Conference on Cyberphysical System. New York, ACM, 2010, 22-31.

[8] LIU Z, LIU J, HE J, et al. Spatio-Temporal UML-Statechart for Cyber Physical Systems[J]. International Conference on Engineering of Complex Computer Systems, 2012, 90(1):137-146.

[9] STEPHAN M, STEVENSON A. A Comparative Look at Model Transformation Languages[EB/OL]. (2013-11-02)[2015-12-1]. cs. queensu. ca/~stephan1projects/836. pdf.

[10] REICHMANN C, GEBAUER D, MULLER-GLASER K D. Model Level Coupling of Heterogeneous Embedded Systems [EB/OL].(2013-10-12)[2015-12-1]. pdf. aminer.org/0001562/512/modus_integrated_oriental_model_for_rapid_prototyping.pdf.

[11] SAKAIRI T, PALACHI E, COHEN C, et al. Model Based Control System Design Using SysML, Simulink, and Computer Algebra System[J]. Journal of Control Science and Engineering, 2013, 2013(1-2): 485380.

[11] PALACHI E, COHEN C, TAKASHI S. Simulation of Cyber Physical Models Using SysML and Numerical Solvers[C]//IEEE International Systems Conference. Orlando, FL: IEEE, 2013:671-675.

[12] CHEN Y X. SteC: A Location-Triggered Specification Language for Real- Time Systems[C]//Proceedings of the 15th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops. Shenzhen, Guangdong: IEEE, 2012:1-6.

[13] 温景蓉,武穆清,宿景芳.信息物理融合系统[J]. 自动化学报,2012,38(4):508-517.
WEN Jingrong, WU Muqing, SU Jingfang. Cyber-Physical Systems[J]. Acta Automatica Sinica, 2012, 38(4):508-517.(in Chinese)

[15] PLATZER André. Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics [M]. Heidelberg: Springer, 2010.

[16] TUO Mingfu, ZHOU Xingshe, AN Li, et al. Research on Safety Verification Technology of Cyber-Physical Systems[C]//The 2nd International Conference on Computer, Intelligent and Education Technology. Guilin: CRC, 2015:525-528.

[17] 朱敏,李必信,陈乔乔,等.基于微分动态逻辑的 CPS 建模与属性验证[J]. 电子学报,2012,40(6):1126-1132.
ZHU Min, LI Bixin, CHEN Qiaoqiao, et al. The-Modeling and Property Verification of CPS Based on Differential Dynamic Logic[J]. Acta Electronica Sinica, 2012, 40(6):1126-1132.(in Chinese)

[18] 周兴社,杨亚磊,杨刚. 信息-物理融合系统动态行为模型构建方法[J]. 计算机学报,2014,37(6):1411-1423.
ZHOU Xingshe, YANG Yalei, YANG Gang. A Method for Cyber-Physical System Dynamic Behavior Modeling[J]. Chinese Journal of Computers, 2014, 37(6):1411-1423.(in Chinese)

[19] 王宇英,周兴社,梁东方. 面向信息物理融合系统的异构模型转换方法[J].西安电子科技大学学报,2015,42(2):108-115.
WANG Yuying, ZHOU Xingshe, LIANG Dongfang. Heterogeneous Model Translation Method for the Cyber-Physical System[J]. Journal of Xidian University, 2015, 42(2):108-115.(in Chinese)

(编辑:徐楠楠)