

面向 CPS 的混成 AADL 建模与模型转换

曹雪岳, 曹子宁, 卜星辰

(南京航空航天大学 计算机科学与技术学院, 江苏 南京 211106)

摘要: 信息物理融合系统(CPS)是将物理过程和计算过程紧密结合的混成系统,是由多个异构的组件通过通信设施联系起来。组合式建模通过对信息物理融合系统组件分别建模,再使用组合机制将组件整合成一个复杂的系统。进程代数经常用于通信系统建模,能够描述进程间的并发关系,但是缺乏对连续变化和随机行为的描述能力。文中在经典进程理论上扩展并提出 CPS 建模语言 HPCCS,同时在模型中使用谓词公式来描述数据间的约束关系。AADL 是目前广泛使用的建模语言,但是缺少连续行为的建模能力,文中结合 HPCCS 扩展 AADL 提出 CPS 系统建模机制 HPCCS-AADL。为了对半形式化的 HPCCS-AADL 进行形式化验证,给出了混成 AADL 到 HPCCS 的转换规则。最后通过飞行控制系统的例子说明提出的混成 AADL 建模能力足够描述 CPS 系统,并且通过模型转换可以转换到形式化的 HPCCS。

关键词: 组合式建模;进程代数;信息物理融合系统;AADL;模型转换

中图分类号: TP301

文献标识码: A

文章编号: 1673-629X(2019)10-0035-06

doi:10.3969/j.issn.1673-629X.2019.10.008

Hybrid AADL Modeling and Model Transformation for Cyber Physical System

CAO Xue-yue, CAO Zi-ning, BU Xing-chen

(School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

Abstract: Cyber-physical system (CPS) is a hybrid system that closely combines physical process and computational process. It is connected by multiple heterogeneous components through communication facilities. Combinatorial modeling is to model the components of CPS separately, and then to integrate the components into a complex system by using composition mechanism. Process algebra is often used in communication system modeling, which can describe the concurrent relations between processes, but lacks the ability to describe continuous changes and random behaviors. We extend the classical process theory and propose the CPS modeling language HPCCS, and use the predicate formula in the model to describe the constraint relation between the data. AADL is a widely used modeling language, but it lacks the ability to model continuous behavior. Therefore, we use HPCCS to extend AADL and propose HPCCS-AADL as the modeling mechanism of CPS system. In order to verify the semi-formal HPCCS-AADL, the conversion rule of hybrid-AADL to HPCCS is given. Finally, an example of flight control system shows that the proposed hybrid AADL modeling capability is sufficient to describe the CPS system and can be converted to formal HPCCS by model conversion.

Key words: combinatorial modeling; process algebra; cyber-physical system; AADL; model transformation

0 引言

信息物理融合系统(cyber-physical system, CPS)^[1]是信息系统和物理设施高度融合和深度协作的新型工业系统。CPS 采用计算、通信和控制结合的 3C 结构^[2],系统不仅包含离散的计算过程,还包含连续的物理事件。CPS 已经广泛应用于航空、医疗、交通

等领域。目前国内对 CPS 的研究方向集中在系统的建模与仿真、网络构建安全性验证上^[3],其中系统的建模是其他研究的基础。目前对 CPS 的形式化建模方法有混成自动机^[4]、微分动态逻辑^[5]、HCSP^[6]等。

体系化结构分析与建模语言(architecture analysis & design language, AADL)^[7]是美国汽车工程协会

收稿日期: 2018-11-12

修回日期: 2019-03-12

网络出版时间: 2019-04-24

基金项目: 航空科学基金(20150652008)

作者简介: 曹雪岳(1993-),男,硕士研究生,CCF 会员(88987G),研究方向为形式化方法;曹子宁,教授,博导,研究方向为形式化方法、人工智能。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20190424.1005.020.html>

SAE 在 2004 年建立的一套适用于嵌入式实时系统的建模规范。AADL 建模语言具备对系统硬件和软件建模的能力,同时能够支持组件建模,可以将组件系统作为软件组件在执行平台的映射。由于 AADL 缺乏形式化语义无法直接对其进行模型检测或者定理证明,文献[8]将 AADL 行为附件转换为实时进程代数 stateful timed CSP,通过模型转换对非线性 F-16 模拟系统进行安全性验证。文献[9]中结合 Z 语言提出了 AADL 非功能属性的形式化描述 Z-AADL,并提出其到 ZIA 的转换规则。文献[10]将 AADL 建模的嵌入式系统模型转换为广义随机 Petri 网,使用广义随机 Petri 网对模型进行性能评价。

进程代数^[11]是作为通信系统描述语言被提出的,可以很好地描述系统中的通信、同步和并发,并且可以使用形式化方法进行推理和验证。进程代数也是学术界研究的热点,各种对经典的进程代数的扩展被提出,如 Timed-CCS、随机进程代数、 π 演算等。同时进程代数可以对 CPS 系统中大量存在的并发与交互给出形式化描述,文献[12]中结合进程代数 CCS 提出一种并发 AADL 用于对 CPS 系统并发特性的形式化建模。

通过分析 CPS 系统的特性,文中在 CCS 的基础上扩展微分方程和概率选择,提出 CPS 系统形式化描述语言 HPCCS。扩展 AADL 行为附件用于描述随机动作并提出混成附件使其能够描述物理环境中的连续变化和组件间通信。由于 AADL 是半形式化的,因此有必要将其转换为形式化语言 HPCCS,根据两者的语法和语义,提出 AADL 到 HPCCS 的转换规则,为 CPS 的形式化验证和分析奠定基础。

1 混成随机进程代数-HPCCS

进程代数最早用来刻画通信系统的行为,可以描述系统的并发特性。文中在 CCS 的基础上提出一种用于 CPS 系统建模的进程代数 HPCCS。HPCCS 能够描述 CPS 系统的连续变化,还可以描述 CPS 系统中存在的概率行为。本节将详细给出 HPCCS 的语法和操作语义,并给出一个水箱的建模案例。

1.1 HPCCS 语法

首先给定一个系统 S , 存在一个动作集合 $A = \{a_1, a_2, \dots, a_n\}$, 系统变量集合分为连续变量集合 $\text{Act}^c = \{c_1, c_2, \dots, c_n\}$ 和离散变量集合 $\text{Act}^d = \{d_1, d_2, \dots, d_n\}$ 。

定义 1: HPCCS 语法。

$P := \varepsilon$ //空进程

$| a. P$ //离散动作

$| \text{lio?}(x). P$ //输入动作

$| \text{lio!}(x). P$ //输出动作

$| d \gg P$ //赋值操作,其中 $d := [v \mid \text{Pr}] \mid [\text{Pr}]$

$| c \blacktriangleright d \gg P$ //流动作, $\blacktriangleright P$ 表示 P 进程可以中断流动作

$| ! (P)$ //递归操作符

$| P \setminus [A]$ //隐藏算子

$| \sum_{i \in I} p_i P_i$ //概率选择

$| P \oplus P$ //交错并发

下面介绍 HPCCS 引入的新的算子的作用。首先赋值操作算子 $d \gg P$, 除了能定义变量值的离散变化也可作为条件约束,表示当 d 中的谓词公式 Pr 满足时继续执行 P 进程。具体形式如下:

$d := [v \mid \text{Pr}] \mid [\text{Pr}]$

其中 v 表示 Pr 中存在赋值操作变量组成的向量,如 $v = \{v_1, v_2, \dots, v_n\}$ 。 Pr 由一组赋值操作和一组变量约束构成,其中赋值操作表示为 $(v_1^+, v_2^+, \dots, v_n^+) = f(v_1, v_2, \dots, v_n)$, 其中 v_i^+ 表示 v_i 变化后的值, f 表示函数;变量约束表示为一组谓词公式, $g(v_1, v_2, \dots, v_n, v_1^+, v_2^+, \dots, v_n^+)$ 可以表示变量间的约束关系,同时也可以约束变量新值需要满足的约束。当 $g(v_1, v_2, \dots, v_n, v_1^+, v_2^+, \dots, v_n^+) = \text{false}$, 即条件不满足,此时进程不执行。当 $g(v_1, v_2, \dots, v_n, v_1^+, v_2^+, \dots, v_n^+) = \text{true}$, 条件执行,并且执行后变量的值用变化后的新值替代,即 $S[v \rightarrow v^+]$, $v^+ = (v_1^+, v_2^+, \dots, v_n^+)$ 。当 d 中没有变量变化,此时 $d := [\text{Pr}]$ 表示进程执行的条件。对于 $d \gg P$, 当 $g(v_1, v_2, \dots, v_n) = \text{true}$ 时执行 P , 否则继续等待条件满足。

流算子 $c := \langle v \mid \text{Pf} \rangle$ 表示进程此时连续变量按照 Pf 中的微分方程变化, Pf 也可以包含对连续变量的约束,当约束不满足时流操作停止执行。右中断算子 $c \blacktriangleright P_2$, 在 c 进程执行时如果 P_2 执行条件得到满足 (d 中的约束满足或者输入输出得到执行), 则执行 P_2 进程, 否则继续执行 P_1 进程。概率选择算子 $\sum_{i \in I} p_i P_i$ 表示当线程执行到这里会产生一次随机选择, 选择一个进程继续执行, 而每个进程的执行概率是由给定权重 p_i 确定的, $p_i / \sum_{j \in I} p_j$ 。交错并发 $P_1 \oplus P_2$, 表示 P_1 和 P_2 进程交错执行。

在定义的进程算子的基础上,通过递归定义引入几个常用算子。首先同步并发 $P_1 \mid [A] \mid P_2 := P_1 \oplus P_2 \setminus [A]$, 表示限制 P_1 和 P_2 只能在 A 动作集同步。然后为 HPCCS 引入顺序操作 $P_1 \odot P_2$, 表示 P_1 执行完继续执行 P_2 。考虑 $P.a$ 这种形式在 HPCCS 中是不能出现的,下面采用递归的形式给出 $P.a$ 的定义:

(1) $P := \varepsilon$, 那么 $P.a := a$;

(2) $P := b.P'$, 那么 $P.a := b.(P'.a)$;

(3) $P := \text{io?}(x).P'$, 那么 $P.a := \text{io?}/i$

$(x).(P'.a);$

(4) $P := d >> P'$, 那么 $P.a := d >> (P'.a);$

(5) $P := \sum_{i \in I} p_i P_i$, 那么 $P.a := \sum_{i \in I} p_i (P_i.a)$ 。

在得到 $P.a$ 后可以定义进程间顺序组合:

$$P_1 \odot P_2 ::= P_1.a! \oplus a?.P_2 \setminus [a].$$

接下来通过水箱系统的例子说明 HPCCS 的建模能力。水箱系统^[13]是由水箱和控制器组成,控制器通过传感器获取水位,根据设定的水位阈值决定是否关闭进水系统。当进水系统关闭时水位由于漏水开始下降。文中在控制器部分引入错误,当水位低于最低值的时候由于控制器故障可能不会打开注水阀门,该故障随机出现,并且出现后可以自动修复,故障率为 20%。模型如下:

WTS := Watertank | [wl, cv] | Controller

Water := $[(v, d) \mid v^+ = v_0; d^+ = d_0] >> [(v = 1) >> [d \mid d' = Q_m - \pi r^2 \times d] \blacktriangleright (wl! (d).cv? (v)) \odot ([v^- = 0] >> [d \mid d' = -\pi r^2 * d] \blacktriangleright (wl! (d).cv? (v)))]$

Controller := $[(v, d) \mid v^+ = v_0; d^+ = d_0] >> !([t \mid t^+ = 0] >> [t \mid t' = 1; t < 10] \odot (wl? (d) \odot [d^- < low] >> Error) \odot [d^- > high] >> v = 1.cv! (v))$

Error := $v = 0.cv! (v) +_{0.8} v = 1.cv! (v)$

1.2 HPCCS 的操作语义

HPCCS 的语义是通过结构化操作语义^[14]规则描述。目前形式化描述语义主要有:操作语义、指称语义、公理语义和代数语义。操作语义是通过抽象的方法描述语言中每个基本算子的执行效果,避免描述的

语言依赖于实现的具体计算机系统,一般使用状态迁移系统描述。该方法的优点在于具有直观的表现形式。

定义 2: 标号迁移系统。

标号迁移系统可以表示为四元组: $M = \langle Q, L, \rightarrow, Q_0 \rangle$, 其中 Q 表示状态集合, L 表示动作集合, $\rightarrow \subseteq S \times L \times S$ 表示状态上的变迁, $Q_0 \subseteq Q$ 表示初始状态集合。

给定一个 HPCCS 进程 S , 可以得到 S 对应的标号迁移系统 $T(P) = \langle Q, L, \rightarrow, Q_0 \rangle$, 构造标号迁移系统的过程如下:

(1) 状态集 $Q = \text{subp}(P) \cup \{\varepsilon\} \times V(S)$, 其中 $\text{subp}(P)$ 表示进程 P 的所有子进程组成的集合, 例如 $P := [t \mid t^+ = 0] >> (\langle t \mid t' = 1 \rangle \blacktriangleright [t > 3] >> P)$, $\text{subp}(P) = \{S, [t > 3] >> P, \langle t \mid t' = 1 \rangle, \varepsilon\} \cup \text{subp}(P)$, ε 表示终止进程。 $V(S) := \{v \mid v \in \text{Var}(S) \rightarrow \text{Val}\}$, 表示每个状态上变量的取值, 其中 Val 表示变量的值域。

(2) L 表示 HPCCS 中的动作, $L := R^+ \cup \text{Channel}.\{?, !\}$. $R \cup \text{Act}$, 由三种动作组成: 时间流逝、通信动作、离散的非通信动作。

(3) \rightarrow 表示状态上的变迁, $\rightarrow := S \times L \times S$ 。

(4) Q_0 表示初始状态, $Q_0 := \{(P, s) \mid s \in V(S)\}$, 其中 P 表示开始时的进程, s 表示此时变量的取值。

定义 3: HPCCS 的操作语义。

下面给出赋值操作 $d >> P$ 、流动作 $c \blacktriangleright d >> P$ 、交错并发算子 $P \oplus P$ 的操作语义。

$$\begin{aligned}
 (1) & \frac{d := [v \mid v^+ = F(v), G(v, v^+)] \text{, 当 } G(v, v^+) = \text{true}}{(d >> P, s) \xrightarrow{\tau} (P, s[v \rightarrow v^+])} \\
 & \frac{d := [v \mid v^+ = F(v), G(v, v^+)] \text{, } \exists d. \forall t. 0 < t \leq d, G(v, v^+) = \text{false}}{(d >> P, s) \xrightarrow{d} (P, s[t \rightarrow t + d])} \\
 (2) & \frac{c = \langle v \mid v' = Pf(v), G(v) \rangle \text{ 如果 } G(v) = \text{false}}{(c, s) \xrightarrow{\tau} (\varepsilon, s)} \\
 & \frac{c = \langle v \mid v' = Pf(v), \exists d > 0. \forall k: k \in [0, d). G(v) = \text{true}}{(c, s) \xrightarrow{d} (c, s[v \rightarrow Pf(v, d), t \rightarrow t + d])} \\
 (3) & \frac{P \xrightarrow{a} P'}{(P \oplus P', s) \xrightarrow{a} (P' \oplus P', s)} \\
 & \frac{P' \xrightarrow{a} P''}{(P \oplus P', s) \xrightarrow{a} (P \oplus P'', s)} \\
 & \frac{P_1 \xrightarrow{a} P'_1, P_2 \xrightarrow{\bar{a}} P'_2}{(P_1 \oplus P_2, s) \xrightarrow{\tau} (P'_1 \oplus P'_2, s)}
 \end{aligned}$$

2 CPS 系统建模工具-混成 AADL

2.1 AADL 组件的抽象描述

行为附件规范可以定义为一个三元组:

$$BA ::= (state_variable, State, Trans)$$

其中 state_varibale 表示系统中定义的变量集合, State 表示系统状态集合, Trans 表示状态中变迁的集合。变迁可以描述为:

$$Tran ::= state1 [guard] \rightarrow state2 \{action\}$$

行为附件规范不能描述状态上的不确定选择。文中在行为附件的基础上引入概率选择的状态集合 transient_State, 引入新的迁移集合 transient_transition。 $transient_transition \subseteq transient_state \times R^+ \times State$, 表示选择状态可以执行一个瞬间选择到一个普通状态, 例如 $t1:tS-[5] \rightarrow S1, t2:tS-[5] \rightarrow S2$ 。提出扩展随机选择的行为附件规范, 定义如下:

定义 4: 带随机选择的行为附件。

带随机选择行为的行为附件, 随机选择状态集合为 Transient_state, 附件规范:

$$PBA ::= (state_variable, State, Transient_state, Trans, Transient_trans), \text{ 其中 } Trans ::= state_1 - [guard] \rightarrow state_2 \{action\}, state_1 \in State, state_2 \in State \cup Transient_state.$$

$Transient_trans ::= state_1 - [p] \rightarrow state_2$, 其中 $state_1 \in Transien_state, state_2 \in State, p$ 表示从 $state_1$ 执行该迁移的权值, 执行概率 $Prob = p / \sum_{t \in Pre(state_1)} (t, p)$ 。

为了使 AADL 能对 CPS 系统中的物理行为建模, 提出基于 HPCCS 的 AADL 混成附件, 利用 HPCCS 流算子对 CPS 中物理行为建模, 利用 HPCCS 的通信操作可以描述计算组件和物理设备间的数据通信。混成附件作为 AADL 设备组件的注解, 对传感器和执行器的连续行为建模或者作为抽象组件实现。混成附件规范由三个部分组成: 变量, 组件的通信接口集合, HPCCS 进程描述的行为集合。

定义 5: 混成附件。

混成附件可以抽象描述为三元组:

$$HA ::= (Variables, Channels, Proc)$$

其中 Variables 表示系统中的变量, Proc 表示由 HPCCS 表示的进程组成的集合, 用于对物理设备建模。Proc 的 BNF 定义如下:

$$Proc ::= process \{ \& process \}$$

$$process ::= identifier \dot{=} expression$$

$$expression ::= \varepsilon \dot{.} expression \mid io? (x') \dot{.} expression \mid$$

$$d' > > expression \mid ! (expression) \dot{.}$$

$$c @ d' > > expression \mid expression ; expression \mid$$

$$r' \dot{.} expression \mid + r' \dot{.} expression \}$$

$$d ::= [(x', x') \mid equation ; guard] \dot{.}$$

$$c ::= < (x', x') \mid flow ; guard >$$

Proc 中 io 只能是混成附件中规定的通道名, 也就是 Channels 中的通道名, Channels 是附件中定义的数据端口。Channels 和 Variables 的定义和行为附件中保持一致。第三节给出混成附件对飞行控制系统建模的例子。

2.2 混成 AADL 到 HPCCS 的转换规则

由于行为附件只会描述系统中的离散行为, 所以转换后的 HPCCS 不包含连续变量和流算子。行为附件可以表示为 $BA = (state_variable, State, Transient_state, Trans, Transient_trans)$, 其中 state_variable 表示行为附件中的变量, 可以对应到 HPCCS 中的离散变量。Trans 表示变迁, 描述了状态间的迁移关系, 可以描述为进程中的动作。转换过程如下:

(1) 将行为附件中的变量映射到 HPCCS 中的离散变量集合中。

(2) 状态集中的状态分别对应一个进程变量。

(3) 行为附件中的迁移可以表示为 $s1 - [guard] \rightarrow s2 \{act\}$ 。其中 guard 有两种形式: on dispatch 和执行条件, 前者表示迁移的周期执行, 后者表示当满足给定条件是迁移执行。所以需要先转换 guard 再转换 act。

(3.1) 转换 guard: 在行为附件中 guard 代表变迁被触发的条件, 一般有三种: 定时触发, 条件触发, 端口上发生的输入输出事件。对于条件触发可以对应 HPCCS 中 d 的谓词形式。端口上的输入输出对应 HPCCS 中的输入输出事件。对于定时触发需要转换为 $! ([t \mid t^+ = 0] > > [t \mid t' = 1] \blacktriangleright [t < T] > > P)$ 。

(3.2) 转换 act, 行为附件 act 中的动作可以转换为 HPCCS 中 d 变量的变化。

(4) 转换行为附件中的 Transient_trans。

3 基于混成系统的飞行控制系统建模

目前国内外先进飞机配置多达数千个嵌入式处理器, 用于进行实时计算任务。这些嵌入式设备通过处理外界物理信息得到各种飞行任务。现代飞行管理系统 (flight management system) 如图 1 所示^[15]。

考虑飞机上升时的操作。首先飞机以平飞的模式到达指定水平位置, 控制器驱动飞机进入上升状态, 开始向上爬升。当达到指定高度后, 控制器驱动飞机进入水平飞行状态。因此上升操作模式可以抽象出三个状态, s_1, s_2 分别代表飞机处于飞机平飞, 上升。使用三个变量 x, y, α 分别描述飞机的水平位置, 垂直位置, 以及飞机的仰角度数。使用常量 V, γ 表示飞行操作规则中定义的常量速度和爬升仰角。假设数据通信是不

可靠的,因此处理器可能会接收不到传感器传来的位置参数,但是在下一次数据传输中可能接收到数据。这种现象以一定概率发生,并且在下次计算时仍然会

以相同的概率触发。图 2 给出了带错误指令的上升操作模式 AADL 行为附件。

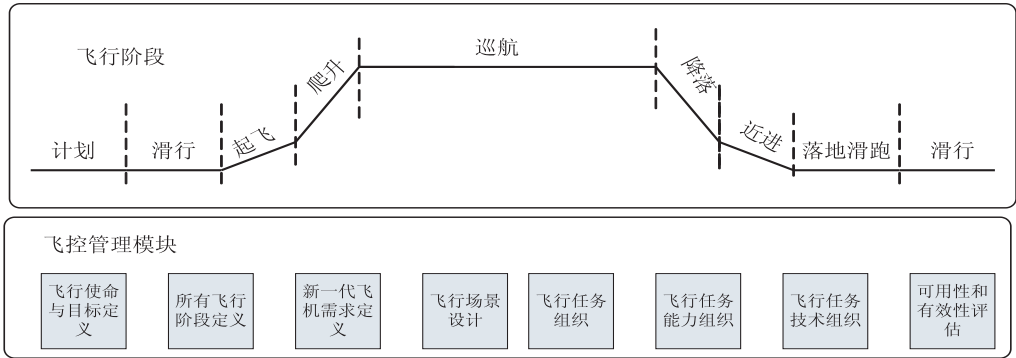


图 1 现代飞行管理系统多阶段示意

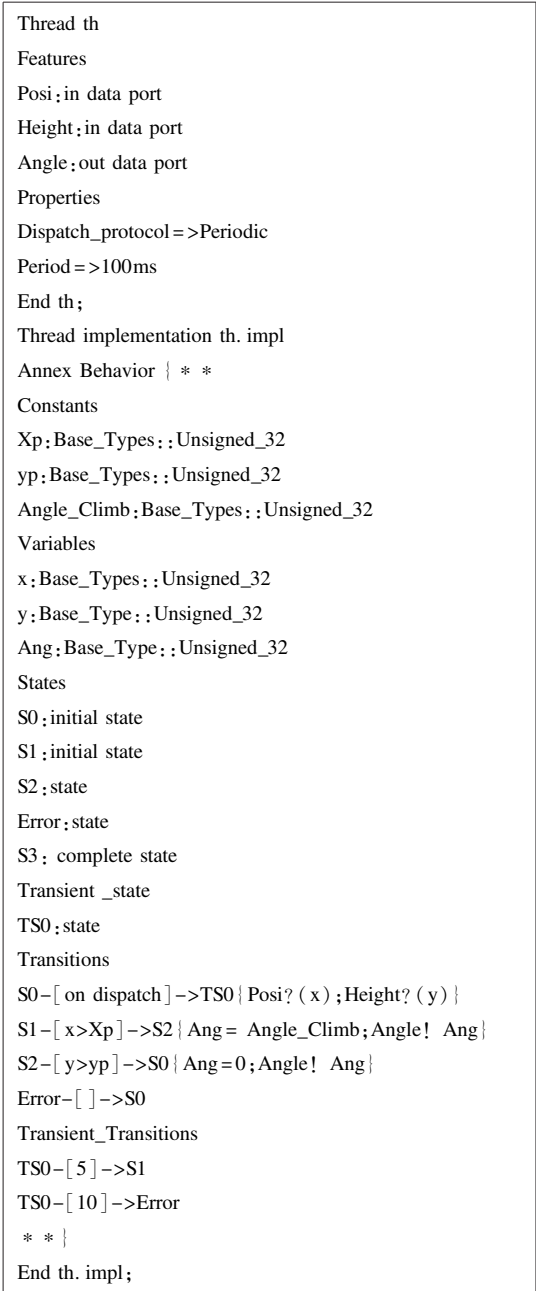


图 2 上升操作模式的 AADL 行为附件

图 3 给出了飞机上升操作模式中物理环境的 AADL 模型。

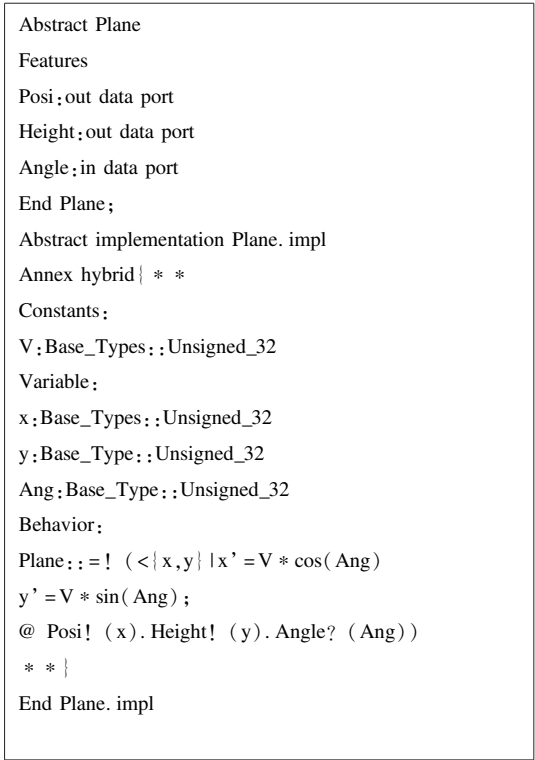


图 3 上升操作模式中的物理信息模型

图 3 用混成附件中的微分方程的形式给出了上升操作模式中状态变量的变化模型。其中 Ang 表示飞机仰角,通过接受 Angle 通道传来的信息进行调整。X,y 分别表示飞机的水平位置和垂直位置信息,通过 Posi、Height 发送给行为附件。

4 结束语

信息物理融合系统是由物理组件和计算组件构成的混杂系统。针对带随机行为的 CPS 系统,在进程代数的基础上扩展随机和混成属性,提出了 CPS 建模语言 HPCCS。HPCCS 具有明确的操作语义,可以应用

模型检测或者定理证明^[16]技术验证是否满足规约。

AADL 是航空系统开发中广泛使用的半形式化建模语言,但是 AADL 在描述物理附件的连续变化时存在不足。文中扩展了 AADL 语言,提出混成附件用于对物理行为建模。通过 AADL 到 HPCCS 的转换机制可以将 AADL 模型自动转换为形式化语言 HPCCS。同时扩展了 AADL 的行为附件使其能够描述信息计算系统中存在的随机行为。该研究为形式化验证 CPS 系统打下基础。基于这套机制可以将更多形式化方法引入 CPS 系统相关研究中。

参考文献:

[1] WOLF W. Cyber-physical systems[J]. Computer, 2009, 42 (3):88-89.

[2] BAHETI R, GILL H. Cyber-physical systems[J]. Computer, 2017, 50(4):14-16.

[3] 温景容,武穆清,宿景芳. 信息物理融合系统[J]. 自动化学报, 2012, 38(4):507-517.

[4] 陈娜,耿生玲,李永明,等. 基于可能性混成自动机的 CPS 建模方法[J]. 西安邮电大学学报, 2016, 21(1):101-105.

[5] 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.

[6] 邹亮. Simulink/Stateflow 模型的形式验证及其应用[D]. 北京:中国科学院大学, 2015.

[7] FEILER P H, LEWIS B, VESTAL S, et al. An overview of The SAE architecture analysis & design language (AADL)

standard: a basis for model-based architecture-driven embedded systems engineering[C]//IFIP world computer congress. [s. l.]: Springer, 2005:3-15.

[8] ZHANG Feng, ZHAO Yongwang, MA Dianfu, et al. Formal verification of behavioral AADL models by stateful timed CSP[J]. IEEE Access, 2017, 5:27421-27438.

[9] 高正,曹子宁. 基于 Z-AADL 模型的形式化转换[J]. 计算机技术与发展, 2017, 27(3):23-28.

[10] 董云卫,王广仁,张凡,等. AADL 模型可靠性分析评估工具[J]. 软件学报, 2011, 22(6):1252-1266.

[11] BERGSTRA J A, PONSE A, SMOLKA S A. Handbook of process algebra[J]. Computer Physics Communications, 2001, 335(2):197-292.

[12] 刘建军,钟珊,叶宏. 基于 AADL 的机载设备系统可靠性建模[J]. 航空计算技术, 2009, 39(2):90-94.

[13] METELO A, BRAGA C, BRANDÃO D. Towards the modular specification and validation of cyber-physical systems[C]//International conference on computational science and its applications. [s. l.]: Springer, 2018:80-95.

[14] COSTA G, STIRLING C. A fair calculus of communicating systems[J]. Acta Informatica, 1984, 21(5):417-441.

[15] 胡军,石娇洁,程桢,等. 一种基于四变量模型的系统安全性建模与分析方法[J]. 计算机科学, 2016, 43(11):193-199.

[16] 肖健宇,张德运,陈海淦,等. 模型检测与定理证明相结合开发并验证高可信嵌入式软件[J]. 吉林大学学报:工学版, 2005, 35(5):531-536.

第 17 届 CCF 全国嵌入式系统大会在西安胜利召开

2019 年 9 月 20-22 日,第 17 届 CCF 全国嵌入式系统大会在西安创新设计中心举行,大会由中国计算机学会(CCF)主办,西安电子科技大学和 CCF 嵌入式系统专委会承办。CCF 嵌入式系统专委会主任吴中海教授、CCF 嵌入式系统专委会秘书长曹喜信教授、中国科学院院士杨孟飞、西安电子科技大学校长杨宗凯、CCF 特派员厦门大学纪荣嵘教授、西安电子科技大学校长助理王泉教授,以及来自全国嵌入式系统领域的 400 余位专家学者出席大会。

大会瞄准嵌入式系统前沿领域,旨在加强嵌入式系统研究领域国内外学者之间的交流与合作,深入探讨相关领域国际发展动态和热点问题,促进我国多学科交叉融合与嵌入式系统产业的发展。会上,邀请杨孟飞院士等 8 位专家分别作了特邀报告;召开了 CCF 嵌入式系统专委会会议;进行了科技成果展示和优秀论文交流。与会人员一致认为要以问题为导向,发扬科学家探索未知前沿的钻研精神,面向国家战略需求和关键核心技术攻关,依托各方优势资源共同推动嵌入式系统研究的全面深入发展,取得丰硕研究成果。