

一种基于事件-响应关系的 Cyber 系统行为模型

宋翠叶 王庆 杜承烈

(西北工业大学计算机学院 西安 710129)

摘要 CPS(Cyber-Physical System)系统中的 Cyber 系统旨在根据用户要求,应用计算、通信和控制等技术实现对现实世界物理行为的精准控制。物理行为是连续和并发的,而 Cyber 行为是离散的,这种异构性给 Cyber 系统行为的分析和设计带来了巨大的挑战,迫切需要一种精确的模型来捕获 Cyber 系统与外界的交互行为语义。按照行为角色的不同,分析了 CPS 系统的抽象组成架构,阐述了各实体的行为;提出了一种基于事件-响应关系的 Cyber 系统行为模型,给出了事件的形式化定义和各类事件的形成规则的语法和语义,对事件的属性取值条件和时序特性进行了详细刻画;在此基础上,定义了事件-响应关系模型的语法和语义;最后以智能探测车为例,分析了该模型在 Cyber 系统设计与开发中的作用,并提出了进一步的研究工作。

关键词 Cyber 系统, CPS 系统, 事件, 系统行为

中图分类号 TP311 **文献标识码** A

Event-Action Behavior Model for Cyber System

SONG Cui-ye WANG Qing DU Cheng-lie

(Department of Computer, Northwestern Polytechnical University, Xi'an 710129, China)

Abstract The cyber part of the cyber physical system is designed to control the behavior of the physical part precisely and timely according to the requirements of the users, employing the cyber abilities such as computing, communicating and control technologies. Physical behavior is time-continuous and concurrent, while the cyber behavior is discrete. Such heterogeneous brings big challenges for the design of the cyber system. An accurate model is needed to capture the interaction requirement of the cyber part and the physical part. First, an architecture of the abstract behavior entities of the CPS system was given and explained. Then an event-action behavior model was proposed and defined in detail. Finally, the effect of the behavior model in the development of cyber system was analyzed in the background of smart detecting vehicle system, and future research work was pointed out.

Keywords Cyber system, CPS system, Event, System behavior

1 引言

CPS 系统是 Cyber 过程和物理过程的有机融合^[1,2]。其中, Cyber 系统是指现在的计算机(尤其是嵌入式计算机)和网络技术,而物理系统是指现实世界的工作设备,如火车道闸、汽车、飞机等。通常在这类系统中,计算机和网络被用于监控物理过程,根据物理系统的反馈进行控制,而物理环境又影响着监控系统的运行,形成闭环控制系统。Cyber 系统的典型行为包括感知物理行为特征值、决策计算和实施对物理对象的控制。在 CPS 系统中,物理行为是连续的、并发的,计算行为是离散的、基于多任务调度的,也就是说,物理行为的发生可能是同时的,而多任务的 CPU 对不同物理行为的响应宏观上是并行的,微观上是穿插串行的,其响应时间是不确定的。这种时间异构性和并发异构性为 Cyber 系统的设计和实现带来巨大的挑战^[3]。建立 CPS 系统的行为模型,捕获 CPS 系统中各实体的行为逻辑和时间特性,是对系统设计进行分

析、验证、代码生成的基础。迫切需要一种精确的模型来捕获 Cyber 系统与外界的交互行为语义并作为 Cyber 系统的行为规格说明,以便于 Cyber 系统的进一步设计和实现。

Cyber 系统行为一般通过以有限自动机^[4]为形式化基础的建模方法来建模,如 UML 状态图。在这种模型中,事件和警戒条件是引发状态迁移的条件,状态则表示行为实体的当前状况。物理实体的行为规律一般可通过时间的函数来表示,如质点运动规律 $s=v \cdot t$ 。可控的物理系统行为一般采用以混成自动机^[5]为形式化基础的混成状态图如 Simulink/Stateflow^[6]等来建模。时间和离散事件共同推进物理行为过程,事件由行为特征变量值穿越阈值引发,事件或警戒条件引发物理行为模式的切换。事件是 Cyber 系统和物理系统行为模型共同采用的驱动概念,以事件为基础,易于建立系统的高层规格说明,也便于将新的实现细节集成到抽象规格模型中^[7]。Cyber 系统与外界的交互关系主要体现为如何根据外部用户输入和感知数据制定响应策略,本文采用事件-响应关

到稿日期:2012-08-10 返修日期:2012-12-26 本文受国家“863”计划基金项目“面向信息-物理融合的系统平台”(2011AA010102)资助。

宋翠叶(1983-),女,博士生,CCF 学生会员,主要研究方向为 CPS 系统建模与验证方法, E-mail: songcy@mail.nwpu.edu.cn; 王庆(1969-),男,博士,教授,博士生导师,主要研究方向为图像处理、计算机视觉和模式识别等; 杜承烈(1970-),男,博士,教授,博士生导师,主要研究方向为复杂实时分布系统的运行支撑环境与分布实时嵌入式软件体系结构。

系来描述该动态交互过程。

在 CPS 事件模型方面,文献[8]首先针对 CPS 系统的时间敏感性和空间分布性提出了时空事件的概念,并在后续研究中对事件组合规则进行改进,形成一种基于概念格的事件模型^[9,10]。文献[11,12]分别结合状态机和事件条件响应(ECA)规则对 CPS 系统行为进行规格描述,采用简单的并操作对事件进行组合。这些定义针对不同的应用目的,对事件属性进行了不同程度的刻画,但在事件内涵和事件组合规则方面较为简单,缺少对事件的属性取值条件和时序组合条件的细致刻画;在事件与响应行为的数量关系方面考虑较少,仅限于一对一的关系描述。

在信息物理交互过程中,事件不仅与相关变量的取值有关,还与变量值在时间轴上的分布有关,甚至不同变量值的特定时序关系形成特定的复杂事件。在 CPS 系统设计过程中,也可能存在多种事件由同一响应行为来处理的情况。本文采用相同的变量值取值时间来刻画物理事件的并发性,引入量化的时序操作符对复杂事件进行刻画,通过“逻辑与”操作符来将多个变量值条件合成完整事件。对于事件与响应的对应关系的描述,提供了事件的“逻辑或”操作符来表示事件与响应之间的多对一关系。通过对事件和事件-响应关系的细致刻画,为 Cyber 系统的行为规格提供了一种精确的建模方法。

本文第 2 节首先对 CPS 系统实体架构进行了阐述,给出了一种 Cyber 系统监控逻辑结构;在此基础上,第 3 节对事件进行了详细的分类,定义并举例说明了事件的属性取值表达方式和不同事件类型的时序组合规则;第 4 节定义了事件-响应关系模型的语法和语义,形成了 Cyber 系统行为模型,并以智能探测车为例分析了该模型在 CPS 系统开发中的作用;最后总结全文。

2 CPS 行为实体架构

如图 1 所示,Cyber 系统由传感器、作动器和计算实体组成。传感器和作动器一般是空间分布的,计算实体一般也是分布式的,它们之间通过网络互连和通信。这里将计算实体抽象为外部事件产生器、感知事件产生器、事件响应处理器和制动事件分发器等 4 个组成部分。

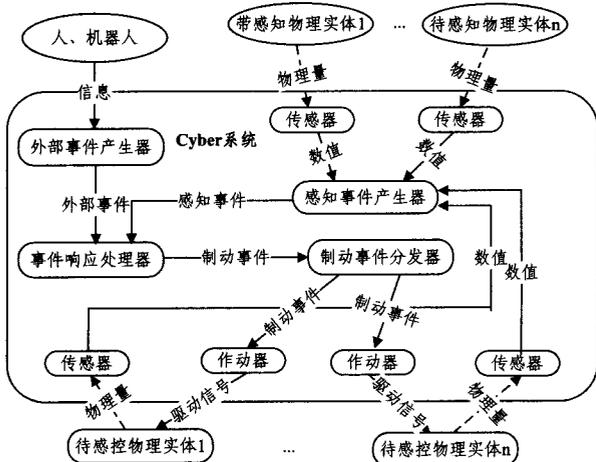


图 1 CPS 系统行为实体架构图

在 CPS 系统中,现实世界的人、自然环境、物理实体等共同构成了 Cyber 系统的外界环境。不同的外部环境与 Cyber 系统之间交互的事件内涵不同。按照与 Cyber 系统的作用关系的不同,Cyber 系统外界环境可分为 3 类:

(1)外部行为实体:主动向 Cyber 系统发送信息的行为实体。如图 1 所示,人或机器人可以按照设计约定,借助 Cyber 系统的接收装置,主动发出输入信息的动作,信息可能是控制命令符号,也可能是基本信息内容,如文本、图像等。Cyber 系统的外部事件产生器接收信息并做出预处理,以事件的方式交由事件响应处理器进行处理。

(2)待感知物理实体:这类实体不主动向 Cyber 系统发送信息,也不受 Cyber 系统的控制,例如风、温度、光、被监护病人等。其物理属性值由 Cyber 系统通过传感器主动感知,以数值形式交由感知事件产生器处理。

(3)待感控物理实体:这类物理实体是 Cyber 系统的嵌入场所,也是 Cyber 系统直接控制的对象,例如智能医疗设备、汽车、飞机等。Cyber 系统通过作动器驱动和控制这类物理实体的行为。

在 Cyber 系统内部,传感器、作动器和事件产生器、制动事件分发器进行协作,由事件响应处理逻辑依据事件的内涵对外部事件和感知事件进行响应,并产生制动事件精确控制待感控物理实体的行为。

3 事件模型

在 CPS 系统行为实体架构中,事件是各行为实体进行交互协作的依据。这里,事件不是简单的协同信号,而是与相关证据相关联的符号表示。例如,由传感器感知而来的数值信息,经过判别、逻辑推理从而形成有意义事件,而事件的时间特性和并发特性也直接影响到控制响应的正确决策。对事件和响应的内涵和时间特性进行准确的描述和建模,对 Cyber 系统中各处理逻辑的设计和实现非常重要。

3.1 事件分类

Cyber 系统与外界的交互依据包括 3 类事件:外部事件 ExternalEvent、感知事件 SensorEvent 和制动事件 ActuatorEvent。另外,Cyber 系统内部的事件处理器的实现可能需要多个计算节点的协同,这里为了事件模型的完备,将多计算节点之间的协同依据表示为 CyberEvent。

事件类型泛化关系如图 2 所示。其中 Event 是最顶层的事件概念,包含所有 Event 类型必须具有的属性。在其 4 个事件子类中,根据其事件形成规则与时间的关系,又可将感知事件 SensorEvent 划分为历史事件 PastEvent、阈值事件 ThresholdEvent 和预测事件 FutureEvent。

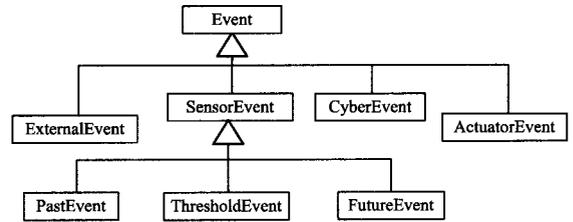


图 2 Cyber 系统事件类型泛化关系图

3.2 事件定义

事件是在系统运行过程中动态产生的,事件的动态特征伴随事件实例的产生而产生。因此采用事件类型 Event Type 和事件实例 EventInstance 分别表示事件的静态属性和动态属性,定义如下:

Event Type= \langle TypeName, Attributes, Rule \rangle

Attribute= \langle StoreType, VarName \rangle

EventInstance= \langle TypeName, EvaluatedTime, Attributes-

Values)

AttributesValue= \langle Attribute, Value \rangle

其中, TypeName 是唯一标识一个 EventType 的字符串, Attributes 是所有与该事件类型相关联的变量组成的集合, 每一个 Attribute 由其存储类型 StoreType 和变量名 VarName 来标识。Rule 是事件的成立条件, 用以判断相关属性值是否构成事件, 不同类型的事件规则描述方法不同。

每一个 EventInstance 除了包括其事件类型名 TypeName 和属性值 AttributesValues 外, 还需要一个唯一的时间戳 EvaluatedTime 与之绑定, 标明该事件的生成时刻。同一次评估周期内生成的事件记为并发事件, 赋予它们相同的 EvaluatedTime 值。

3.3 事件形成规则 Rule 定义

不同类型的事件, 其属性集合模型相同, 但事件形成条件不同, 下边分别对它们进行分析和定义。

1) ExternalEvent 和 CyberEvent 事件规则。这两类事件规则都可采用含变量值的等式表达式的布尔逻辑来表示, 例如对于外部按钮事件, 代表按钮输入值的变量为 int 型变量 choice 和 string 型变量 account。与该属性值关联的事件类型 Type1 的事件规则为 Rule1:

Rule1: $(choice == 1) \& \& (account != "")$

这类事件规则语法与 C 语言类似, 但只涉及变量值之间的比较或变量值与常量的比较, 不涉及复杂的计算过程。

2) SensorEvent 规则。按照事件的形成规则, 3 类感知事件对应 3 种不同的形成规则:

a) 阈值事件规则 TRule。TRule 是 ThresholdEvent 的判定依据。阈值是与被监视变量关联的已知设定值。设变量 x 关联的阈值 TH_x , 阈值穿越事件规则定义为:

TRule $\rightarrow x \text{ opera } TH_x$
opera $\rightarrow < | \leq | > | \geq | = | \neq$
TRule $\rightarrow TRule \wedge TRule$

其中, 变量值与阈值的大小比较关系构成了基本的阈值事件, 多个阈值事件的与连接构成复合阈值事件。例如, 某温度阈值事件类型记为:

$\langle \text{highEvent}, \{ \text{tempInside}, \text{tempOutside} \}, \text{Rule2} \rangle$

其中, 两个温度变量 tempInside 和 tempOutside 分别表示室内、外温度, 则其阈值事件规则表示为:

Rule2: $\text{tempOutside} \leq 0 \wedge \text{tempInside} > 25$

该事件用于表示冰天室内温度过高的情况。这里拒绝或逻辑, 若多种事件对应的系统响应相同, 则将其描述在事件-响应关系模型中。

b) 历史事件规则 PRule。PRule 为 PastEvent 的判定依据。与阈值事件相比, 历史事件的形成不仅与检测变量值的当前取值相关, 还与被检测变量值在过去一段时间内的取值有关。规则 PRule 定义为:

PRule $\rightarrow \text{TimeInterval } H | P \text{ TRule}$
PRule $\rightarrow \text{TimeInterva } TRule \text{ Prev} | \text{Since } TRule$
PRule $\rightarrow PRule \wedge PRule$
TimeInterval $\rightarrow [min, max]$

这里引入了线性时序逻辑 LTL 逻辑操作符 H、P、Since 和 Prev^[13,14], 并采用 $[min, max]$ 的形式对操作符进行时间区间量化^[15], 以描述基于历史监控数据的事件推导规则。这里时间区间总是以当前评估时刻为原点, min 和 max 表示区间

距离原点的距离值。min 的最小取值为 0, max 的最大取值由 MAX 表示, 其随具体应用而定, 用于限定规则的合法性。4 个逻辑操作符的时间量化语义分别描述如下:

$[min, max]H \text{ tr} : \forall t \in [min, max], \text{tr} = \text{true}$
 $[min, max]P \text{ tr} : \exists t \in [min, max], \text{tr} = \text{true}$
 $[min, max]tr_1 \text{ Prev } tr_2 :$
 $\exists t_1 \in [min, max], tr_1 = \text{true}$
 $\wedge \exists t_2 \in [min, max], tr_2 = \text{true}$
 $\wedge t_1 > t_2$
 $[min, max]tr_1 \text{ Since } tr_2 ;$
 $\exists t_2 \in [min, max], tr_2 = \text{true}$
 $\wedge \forall t_1 \in [min, t_2], tr_1 = \text{true}$

通过对时间的区间量化语义和线性逻辑操作符自身的量词语义, 可以准确地对历史事件进行刻画。例如在某瓦斯浓度的监控系统中, 瓦斯突变预警事件记为:

$\langle \text{guardEvent}, \{ \text{density} \}, \text{Rule3} \rangle$
该历史事件的形成规则表示为:
Rule3: $\text{density} \geq 0.006 \wedge [0, 2] P \text{ density} \leq 0.003$

事件 guardEvent 表示在最近的两个感知采样区间内, 瓦斯浓度发生了从 0.3% 到 0.6% 的突变。

c) 预测事件规则 FRule。FRule 是预测事件的判定依据。预测事件是指根据当前感知信息, 计算推测出来的事件, 如船只将在 60s 内触到障碍物, 或车身将在 3s 内倾倒等。这类事件的产生本质是对物理实体行为的预估, 描述方法 FRule 定义如下:

FRule $\rightarrow \text{TimeLength } TRule$
FRule $\rightarrow FRule \wedge FRule$

其中, TimeLength 表示事件的发生时刻距离当前时刻的预估时间。例如某翻车预测事件为:

$\langle \text{turnOverEvent}, \{ \text{angle} \}, \text{Rule4} \rangle$

其中, angle 表示车辆与地面夹角, Rule4 可表示为:

Rule4: $3 \text{ angle} = 0$

当多个 TRule 事件的组合才会触发 Cyber 系统响应时, 则用它们的与连接来组合为单一 FRule 事件。

3) 制动事件规则 ARule; 与其他类型的事件不同的是, 其他事件的形成规则是读取属性值和推理的过程, 而制动事件是属性值写的过程。规则定义如下:

WRule $\rightarrow y = \text{newValue}$
WRule $\rightarrow \text{WRule } \text{Next } tVal \text{ WRule}$
ARule $\rightarrow \text{ExecTInterval } WRule$
ExecTInterval $\rightarrow [min, max]$
ARule $\rightarrow ARule \wedge ARule$

规则中, WRule 表示简单的制动命令和命令的顺序连接, Next tVal 表示一事件执行后, 间隔 tVal 再执行另一个 WRule。在 WRule 基础上附加了制动事件的执行时间区间, 形成了完整的 ARule。WRule 的与连接表示需要并行被执行。这里, 执行时间 $[min, max]$ 是以事件产生时刻为原点的, 限定了制动事件的精准范围, 只要事件的执行起始时间在该范围内, 都认为控制是精准的。例如汽车行走控制事件, 30s 以后, 前后不得超过 1s, 车身右转 90°, 转向完成后, 向前行进 20s, 停车。事件记为:

$\langle \text{runActuatorEvent}, \{ \text{arc}, \text{stop} \}, \text{Rule5} \rangle$
规则描述为:

4 Cyber 行为规约模型

4.1 事件-响应关系

事件模型为 Cyber 系统与外界的交互依据进行了刻画,事件-响应模型则用于对 Cyber 系统响应逻辑进行规约,是图 1 所示事件响应处理器的实现依据。响应行为表示为:

$$\text{ReactionBehavior} = \langle \text{Events}, \text{Actions}, \text{CausalLogics} \rangle$$

其中,Events 为事件处理器在一次事件处理周期中面临的所有事件集合,Actions 为事件处理器需要执行的行为动作集,每一个 Action 对应于一个或多个事件。Action 定义为:

$$\text{Action} = \langle \text{ActionName}, \text{Description}, \text{OutputEvents} \rangle$$

其中,ActionName 为一个特定计算行为的唯一标识符,Description 为该 Action 行为语义的文本描述,OutputEvents 则用于表示该响应函数的输出事件,一般为 CyberEvent 或 ActuatorEvent 类型,用于和其他计算实体协同或控制物理实体。

CausalLogics 表示各个 Event 与 Action 之间的响应逻辑关系。CausalLogic 定义如下:

$$\text{CausalLogic} \rightarrow \text{if EvCond then ActionName}$$

$$\text{EvCond} \rightarrow \text{EventType}$$

$$\text{EvCond} \rightarrow \text{EvCond} \vee \text{EvCond}$$

$$\text{CausalLogics} \rightarrow \text{CausalLogic} \wedge \text{CausalLogic}$$

EventType 代表某事件的发生,不同事件的或连接用于表示多个事件对应相同 Action 的逻辑关系,CausalLogics 的与连接,则表示两个或多个响应行为需要被同时执行。

4.2 应用分析

本节以某智能探测车为例,对其自主行走和自主避障过程中 Cyber 系统行为进行分析和事件响应关系进行建模,进而对 ReactionBehavior 模型在 Cyber 系统开发过程中的作用进行分析和探讨。

假设智能探测车在其工作环境中需要自主感光充电,感知路径近距离障碍,计算车身姿态,当监测到电量不足时,需要自主调整工作模式进入休眠状态,当感知前方障碍或车身即将倾倒下时,则执行刹车命令。在该应用中,事件类型集 Events 表示为:

$$\langle \langle \text{evPowerWeak}, \{ \text{electricity} \}, \text{electricity} \leq 0.1 \rangle \rangle;$$

$$\langle \langle \text{evObstacleClose}, \{ \text{location} \}, \text{location} \leq 5 \rangle \rangle;$$

$$\langle \langle \text{turnOverEvent}, \{ \text{angle} \}, 3 \text{ angle} = 0 \rangle \rangle;$$

$$\langle \langle \text{evStop}, \{ \text{velocity} \}, [0, 2] \text{ velocity} = 0 \rangle \rangle$$

该事件模型当中, evPowerWeak 和 evObstacleClose 属阈值事件; turnOverEvent 属预测事件,表示 3s 之内车身会倒;而 evStop 为作动事件,表示 2s 之内车身要停止运动。变量 electricity 用于表示感知到的电量剩余比例值, location 表示感知到的前方障碍距离值,单位为 m; angle 表示车身的倾斜与地面形成的夹角度,最后 velocity 表示期望的速度值,单位为 m/s。事件模型精确地捕获了事件的内涵。

该案例涉及到的响应动作集 Actions 定义如下:

$$\langle \langle \langle \text{sleep}, "change the mode to sleep", \{ \} \rangle \rangle;$$

$$\langle \langle \langle \text{stop}, \text{stop the vehicle}, \{ \text{evStop} \} \rangle \rangle \rangle$$

响应逻辑模型 CausalLogics 如下:

$$\{ \text{if evPowerWeak then sleep};$$

$$\text{if turnOverEvent} \vee \text{evObstacleClose then stop} \}$$

至此,捕获了智能探测车与外界的交互语义,建立了完整的 Cyber 行为模型。该模型对于 Cyber 系统实现的主要作用

有:1)事件模型为事件产生逻辑和事件响应逻辑提供了精确的规约;2)响应集 Actions 可作为 Cyber 响应逻辑的进一步开发的接口;3)事件的时间特性被准确地捕获,为 Cyber 行为的合时正确性分析提供了模型依据。

结束语 针对 CPS 系统中 Cyber 系统与外界环境的交互关系建模需求,提出了一种事件-响应关系模型,采用事件和响应分别表示 Cyber 系统与外界的交互依据和其自身的响应行为。对交互事件进行了分类分析,给出了各类事件的形式化定义;并将感知事件按照产生规则与时间的关系划分为历史事件、阈值事件和预测事件,分别定义了其产生规则。以智能探测车为背景阐述了事件-响应关系模型的建模过程。该模型为 Cyber 系统的进一步开发提供了重要的形式规约,实现该规约模型向实现模型的自动转换是进一步的研究工作。

参考文献

- [1] 何积丰. Cyber-physical systems[J]. 中国计算机学会通讯, 2010, 6(1): 25-29
- [2] Lee E A. Cps foundations[C]// Proc. of the 47th Design Automation Conference, DAC'10. New York, USA, ACM, 2010: 737-742
- [3] Derler P, Vincentlli A S. Modeling cyber-physical systems[J]. Proc. of the IEEE (special issue on CPS), 2012, 100: 13-28
- [4] Hoperoft J E. 自动机理论、语言和计算导论(第 2 版)[M]. 刘田, 等译. 北京: 机械工业出版社, 2004: 25-56
- [5] van der Schaft A, Schumacher H. 混成动态系统引论 [M]. 宋永华, 等译. 北京: 清华大学出版社, 2007: 5-13
- [6] 刘杰. 基于模型的设计及其嵌入式实现[M]. 北京: 北京航空航天大学出版社, 2010: 141-167
- [7] Talcott C. Cyber-Physical Systems and Events[C]// Software-Intensive Systems: Software-Intensive Systems and New Computing Paradigms. Springer-Verlag Berlin, Heidelberg, 2008: 101-115
- [8] Tan Y, Vuran M C, Goddard S. Spatio-temporal event model for Cyber-Physical Systems[C]// Proc. of 29th IEEE International Conference on Distributed Computing Systems Workshops. 2009
- [9] Tan Ying, Mehmet C V, Steve G. A concept lattice-based event model for cyber-physical systems[C]// Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS '10. 2010: 50-60
- [10] Yue Ke, Wang Li, Ren Shang-ping, et al. An adaptive discrete event model for cyber-physical system[M]. The Analytic Virtual Integration of Cyber-Physical Systems Workshop, 2010
- [11] Chen Li-na, Huang Hong-bin, Deng Su. Research on CPS Spatio-Temporal Event Model based on the State[C]// Proc. of The 6th International Conference on Computer Science & Education. 2011: 195-198
- [12] Klein R, Xie Jing-quan, Usov A. Complex events and actions to control cyber-physical systems[C]// Proc. of 5th ACM International Conference on Distributed Event-Based Systems, DEBS' 11. 2011: 29-37
- [13] Bellini P, Mattolini R, Nesi P. Temporal logics for real-time system specification[J]. ACM Comput. Surv., 2000, 32(1): 12-42
- [14] Furia C A, Mandrioli D, Morzenti A, et al. Modeling time in computing: A taxonomy and a comparative survey[J]. ACM Comput. Surv., 2010, 42(2): 1-59
- [15] Yu Y, Ren S, Frieder O. Interval-based timing constraints their satisfactions and applications[J]. IEEE Transactions on Computers, 2008, 57(3): 418-432