

信息物理融合系统的软件需求分析

刘 春¹⁾ 黄冉冉¹⁾ 张 伟^{2),3)} 赵海燕^{2),3)} 金 芝^{2),3)}

¹⁾(河南大学计算机与信息工程学院 河南 开封 475001)

²⁾(高可信软件技术教育部重点实验室(北京大学) 北京 100871)

³⁾(北京大学信息科学与技术学院软件研究所 北京 100871)

摘 要 计算过程与物理过程的融合使得信息物理融合系统(Cyber-Physical Systems, CPS)的软件需求分析成为一个具有挑战性的任务. 首先, 分析人员需要从用户所期望实现的物理实体变化出发, 基于对物理实体性质的认识来推理分析软件需求; 其次分析人员已不能将 CPS 中的软件看成一个整体去描述它的外部行为, 而需要分析 CPS 所应包含的各个软件实体和物理实体, 描述每个物理实体的性质和软件实体应具有的行为; 还有计算过程与物理过程的融合也使得分析人员必须采取一种统一的方式来描述物理实体的性质和软件实体的行为, 以方便用户需求的满足性验证. 基于问题框架方法和面向目标方法, 作者提出了一种适合于 CPS 的软件需求分析方法. 该方法采用现象间的因果关系式这一具体形式来统一描述 CPS 中物理实体的性质和软件实体的需求, 然后从用户所期望的物理现象出发, 遵循面向目标的方法, 将 CPS 软件需求的分析过程转化为建立满足用户需求的现象间因果关系链的过程, 最后通过基于 Alloy 的目标现象可达性验证来检验用户需求的可满足性; 并且用一个自适应巡航控制系统的案例来说明所提方法的可行性.

关键词 信息物理融合系统; 软件需求; 面向目标的方法; 问题框架方法

中图法分类号 TP311 **DOI 号** 10.11897/SP.J.1016.2016.02344

Analyzing Software Requirements for Cyber Physical Systems

LIU Chun¹⁾ HUANG Ran-Ran¹⁾ ZHANG Wei^{2),3)} ZHAO Hai-Yan^{2),3)} JIN Zhi^{2),3)}

¹⁾(School of Computer and Information Engineering, Henan University, Kaifeng, Henan 475001)

²⁾(Key Laboratory of High Confidence Software Technologies of Ministry of Education (Peking University), Beijing 100871)

³⁾(Institute of Software, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871)

Abstract The integration of computing process with physical process makes the software requirements analysis for Cyber-Physical Systems (CPS) a challenging task. First, software requirements need to be derived from the desired changes of physical entities and the properties of such physical entities. Second, analysts can't treat the software as a whole and describe its external behaviors. Instead, they need to analyze the software entities and physical entities composing CPS and capture the properties of each physical entity and desired behaviors of each software entity. Finally, a unified way is required to describe the properties of physical entities and the behaviors of software entities to help validate the satisfaction of user' requirements. Based on problem frame and goal oriented approaches, this paper proposes an approach to address this task. It describes the properties of physical entities and the behaviors on software entities in CPS as the causal relations between

收稿日期:2015-05-26;在线出版日期:2016-03-08. 本课题得到国家自然科学基金(91318301,61300035,61402150)、中国博士后基金(2014M552000)、北京大学高可信软件技术教育部重点实验室开放课题(HCST201301)及河南省教育厅重点研究项目(14A520009)资助. 刘 春,男,1982 年生,博士,讲师,主要研究领域为需求工程. E-mail: liuchun@henu.edu.cn. 黄冉冉,女,1989 年生,硕士研究生,主要研究领域为需求工程. 张 伟,男,1978 年生,博士,副教授,主要研究领域为需求工程和软件复用. 赵海燕,女,1966 年生,博士,副教授,主要研究领域为软件工程和领域工程. 金 芝,女,1962 年生,博士,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为需求工程、知识工程、基于知识的软件工程.

phenomena. Starting from the physical phenomena desired by users, it then follows the goal based analysis process, transforms the software requirements analysis into building the phenomena causal chains required to meet users' requirements, and finally validates the satisfactions of users' requirements by checking whether the desired phenomena in the causal chains can be reached through describing the causal chains with Alloy. An adaptive cruise control system has been taken as an example to show the feasibility.

Keywords cyber physical systems; software requirements; goal oriented approach; problem frame approach

1 引言

信息物理融合系统(Cyber-Physical Systems, CPS)是一个既包含物理实体又包含软件实体,并将计算过程和物理过程融合在一起的混合系统^[1-2].它一般由多个嵌入式系统通过网络连接起来,与传统的软件系统和嵌入式系统有很大不同.首先,CPS中的软件实体主要用来感知和控制物理实体,因此软件的需求更多的体现为用户所期望实现的物理实体变化,比如汽车速度的控制或者火灾的及时报警,而不是传统软件需求所关注的软件行为的变化.其次,CPS一般会包含多个互联的软件实体,而不是仅仅由一个软件实体来实现所有的控制逻辑,这些软件实体在系统运行过程中又感知和控制了更多的物理实体,因此CPS比传统封闭的嵌入式系统更为复杂.

在这种情况下,CPS的软件需求分析就成为一个具有挑战性的任务.一方面,CPS的软件需求需要从用户所期望实现的物理实体变化出发,基于对物理实体性质的认识来进行推理才能得到;另一方面,CPS的软件需求分析已不能将CPS中的软件看成一个整体去描述它的外部行为,而是需要分析CPS应该包含哪些软件实体和物理实体,为什么需要这些实体,它们之间的关系是什么以及每个物理实体所具有的性质和软件实体应具有的行为.还有,物理过程与计算过程的融合使得如何采取一种统一的方式来描述物理实体的性质和软件实体的行为以方便用户需求的满足性验证,也成为必须要考虑的问题.

当前,问题框架方法^[3]将一个软件开发问题分为三部分:软件、现实世界和用户需求,主张从用户需求出发,基于对现实世界的认识来推理分析软件需求,通过将CPS的物理实体看作问题框架方法中

的现实世界,问题框架方法可以为CPS的软件需求推理提供一种分析框架.它告知了分析人员应该从哪里开始进行分析以及如何处理物理实体在软件需求分析中的作用.但是,该方法缺乏由用户需求推理分析软件需求的有效方法.而面向目标的方法^[4]以目标来表达用户需求,以与/或分解来将抽象的用户需求操作化为具体的软件需求,因此可以为从用户需求出发推理分析CPS的软件需求提供一种结构化的方法.但是,对于从哪里开始目标分解和如何进行目标分解,该方法却具有一定随意性.

本文基于问题框架方法与面向目标方法,提出一种适合于CPS的软件需求分析方法.该方法融合问题框架方法和面向目标方法的优点,并根据CPS的特点进行相应的扩展来分析CPS的软件需求.一方面,该方法从用户期望的各种物理现象出发,将用户需求作为高层的目标,然后按照面向目标的方式来推理软件需求,分析构成CPS的软件实体、物理实体以及物理实体的性质、软件实体的需求和各个实体之间的关系;另一方面,以现象间的因果关系式这一形式来统一描述物理实体的性质和软件实体的需求,将面向目标的需求分析过程转化为建立满足用户需求的现象间因果关系链的过程,展现物理过程与计算过程的融合.最后,为了验证用户的需求的可满足性,该方法利用Alloy^[5]来描述物理实体的性质和软件实体的行为需求,通过验证目标现象的可达性来检测用户需求的可满足性.本文利用一个自适应巡航控制系统展示了该方法的可行性.

本文第2节是对本文所使用的自适应巡航控制系统这一案例、问题框架方法、面向目标方法和Alloy语言等背景知识的介绍;第3节从概念框架和基本过程两个方面概述本文方法;第4节结合案例来详细说明本文方法的具体过程;最后是相关研究工作介绍以及对本文的总结.

2 背景知识

2.1 案例:自适应巡航控制系统

对驾驶员来说,如果在驾驶过程中长时间地集中注意力,将会很疲劳,因此他们希望有一个系统可以帮助他们自动地维持车辆的速度,尤其是在高速公路上.当前方没有车辆时,控制车辆以巡航速度行驶;当前方有车辆时,采用跟踪模式,控制车辆与前方车辆保持安全距离(安全距离一般指的是汽车紧急刹车时从刹车到停止所需要的一个最短时间 T ,因此保持安全距离可以认为是保持比率 d/v 小于等于 T ,其中 d 为在前车存在的情况下两车的间距, v 为被控车辆的行驶速度)^①.

以上就是用户对于自适应巡航控制系统的需求.为了实现该需求,整个自适应巡航控制系统需要一系列诸如巡航控制器、测速器等软件实体以及刹车、引擎等物理实体.因此,自适应巡航控制系统是一个典型的信息物理融合系统.本文将以该系统为案例来详细说明本文所提出的方法.

2.2 问题框架方法

问题框架方法由 Jackson 于 20 世纪 90 年代提出^[3].该方法认为用户对软件的需求存在于软件的运行环境之中,表达的是用户期望的环境现象,而最终所建立的软件系统必须通过影响环境来满足用户的需求.因此,该方法认为一个软件问题包含三部分:软件 S 、现实世界 W 、用户需求 R ,三者满足如下的关系:

$W, S \vdash R.$

其中软件 S 是用户想要开发的软件系统,现实世界 W 是已存在的软件运行环境,由一组领域实体构成, $\vdash$ 表达的是当软件 S 安装于现实世界 W 之后能够使得用户需求 R 得到满足.

基于上述认识,问题框架方法强调基于对现实世界性质的刻画来由用户需求推理分析软件的需求.实际中,分析人员可以使用任何语言来描述一个软件问题(描述 W 、 S 、 R).通常,问题框架方法使用图 1 所示的问题图来展示一个软件问题(该问题图以本文案例为例,并且假设雷达、ECS 等软件实体是已存在于现实世界中的领域实体,所要开发的软件只是巡航控制器).

如图 1 所示,问题图展现了用户需求、用户需求所引用的环境现象、构成软件运行环境的领域实体、

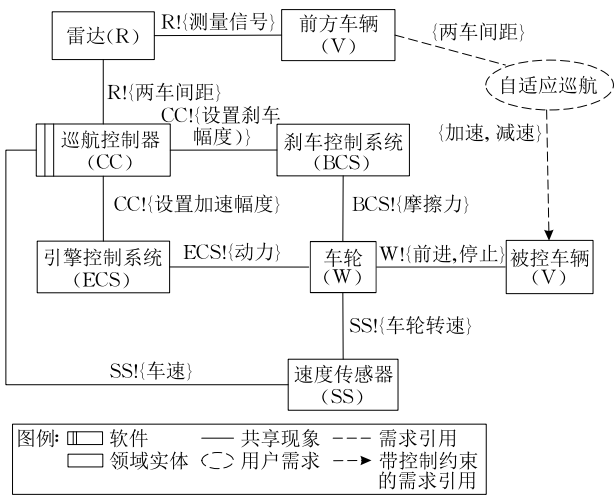


图 1 问题框架方法的问题图

软件与领域实体以及领域实体与领域实体之间的关系.实体(包括软件与领域实体)间的连接线表示共享现象(连接线上的大括号),一个共享现象可以是事件、值或者状态,而大括号的前缀(例如 $R!$)表示共享现象的双方中的一方对现象的触发或者控制作用.本文将以问题图来表示 CPS 的结构模型,即构成 CPS 的实体以及实体之间的关系.

2.3 面向目标的方法

面向目标的方法是一种结构化的软件需求分析方法.它以“目标”来表达用户对软件的需求,通过与/或分解将抽象的用户需求操作化为具体的软件任务,形成一个由用户需求到软件需求的树形结构.在该结构中,高层目标代表低层目标存在的原因,而低层目标则反映满足高层目标的手段.因此,该方法不仅可以回答需求分析过程中关于某个需求“Why”的问题还可以回答“How”的问题.

当前,研究人员已提出了不同的目标模型来指导面向目标的需求分析.图 2 展示了 Jureta 等人^[4]所提出的目标模型(以本文案例为例).它包含了目标、领域假设、任务等概念.其中,目标(以字母 G 标注的矩形表示)表达用户对系统的功能需求;任务(以字母 T 标注的矩形表示)表达软件系统的一个活动;领域假设(以字母 K 标注的矩形表示)则表示人们对环境中的各种现象的认识或者对现象所具有性质的刻画;而蕴含关系(以空心的小圆圈表示)是一种满足关系,即一个目标的满足可以通过其他目标的满足、其他任务的执行或者领域假设的成立来

① http://sunnyday.mit.edu/safety-club/workshop5/Adaptive_Cruise_Control_Sys_Overview.pdf

实现. 本文以图 2 所示的目标模型来组织和表达 CPS 的软件需求分析的具体过程.

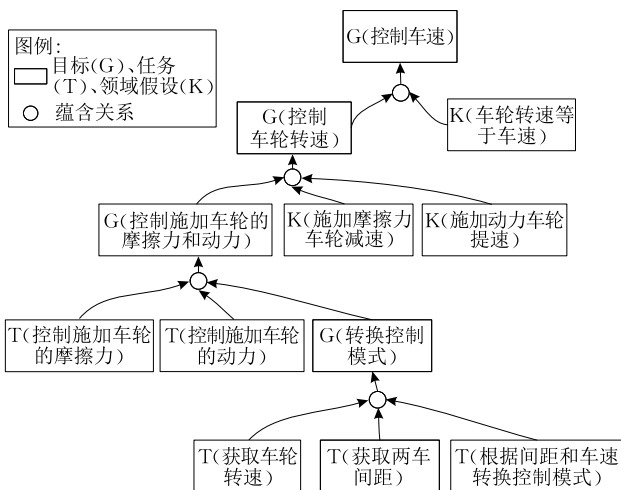


图 2 Jureta 等人提出的目标模型

2.4 Alloy

Alloy 是由 MIT 软件设计小组基于一阶逻辑和集合论所设计的一种描述性的、面向对象的、轻量级形式化建模语言^[5]。它提供的申明性语法便于分析人员建立软件系统的行为和结构模型, 并且 Alloy 分析器能够以可视化的方式展现模型的反例. 因此本文选择基于 Alloy 来验证所建立的软件需求模型. 在应用过程中, 本文将构成 CPS 的每个实体(物理实体或软件实体)作为一个对象, 然后采用 Alloy 来定义该对象并通过建立现象间的因果关系式来描述物理实体的性质或者软件实体的需求, 最后应用 Alloy 分析器来验证用户期望现象的可达性, 并以此来检测用户需求的可满足性.

3 方法概述

根据问题框架方法, 一个 CPS 的开发问题可以认为包括如下三部分: 一组用户需求 R 、一组物理实体 D 和一组软件实体 S . 每个实体都具有特定的性质 P , 其中软件实体的性质即是人们对软件实体的需求. 系统开发的主要任务就是要构建具有相应性质的物理实体集合 D 和软件实体集合 S , 并且通过这些实体在实际中表现出应有的性质来满足用户的需求 R . 基于此, 本文方法旨在帮助系统分析人员完成如下两个任务:

(1) 软件需求推理: $f: R \rightarrow P(D \cup S)$.

(2) 用户需求验证: $P(D \cup S) \Rightarrow R$.

软件需求推理就是从用户需求 R 出发, 推理分

析构成 CPS 所需要的物理实体 D 、软件实体 S 以及它们所应具有的性质 $P(D \cup S)$. 用户需求验证则是在软件需求推理之后, 验证基于所识别的物理实体和软件实体的性质, 用户需求是否能够得到满足, 即 $P(D \cup S) \Rightarrow R$ 是否能够成立.

3.1 概念框架

本文方法的概念框架如图 3 所示. 本文认为 CPS 由各个实体组成. 实体是 CPS 中客观存在的, 能够完成特定功能的组件. 它可以是软件实体, 也可以是物理实体. 软件实体是需要编程实现, 包括相应运行平台在内的计算实体. 实际中, 软件实体根据其功能又可以进一步分为感知、分析、控制等类型的软件实体. 而物理实体是相对于软件实体而存在的非计算实体. 它往往是软件实体监控的对象. 一个软件实体可以包含多个软件实体和物理实体, 而一个物理实体只可以包含多个物理实体.

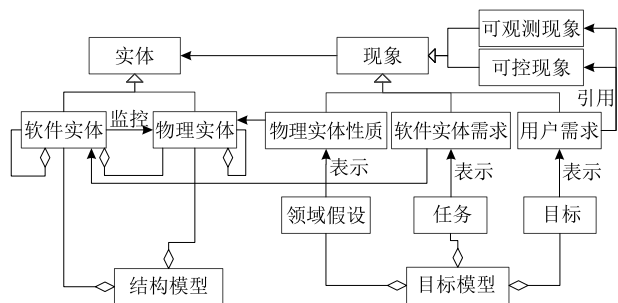


图 3 本文方法的概念框架

在 CPS 的运行过程中, 每个实体都表现一定的现象. 现象是一个实体在与其他实体相互作用的过程中其内在性质的外在表现, 可以是事件、值或者状态; 而对实体性质的描述往往通过对其现象的描述来实现. 其中物理实体性质描述的是物理实体在与其他实体交互过程中所表现出来的现象; 软件实体需求描述的是软件实体在与其他实体交互过程中所应具有的现象, 即软件实体需要实现的现象.

物理实体现象和软件实体现象的融合形成 CPS 的现象, 而用户需求就是通过引用这些现象来表达 CPS 应具有的功能, 所以用户需求描述的也是现象, 是由物理实体现象和软件实体现象融合而成的复合现象. 一般来说, 用户需求所引用的实体现象可分为如下两类: 可观现象, 是 CPS 需要感知的现象, CPS 可以通过一些方法直接或间接地感知; 可控现象, 是 CPS 需要控制或者实现的现象, 是目标现象. 一个现象可以既是可观现象又是可控现象, 例如巡航控制系统中汽车的速度这一现象.

本文方法的目的是建立 CPS 的结构模型和目标模型. 结构模型反映构成 CPS 的软件实体、物理实体及其关系. 通过将用户需求、软件需求以及物理性质分别表示为“目标”、“任务”和“领域假设”, 图 2 所示的目标模型被用来表示 CPS 的各个实体的现象以及它们与用户需求之间的关系. 结构模型和目标模型的具体表示方式将在第 4 节进行详细介绍.

3.2 基本过程

如图 4 所示, 本文方法的基本过程包括三步: 明确用户需求、推理软件需求和验证用户需求的可满足性.

首先, 明确用户需求. 这里用户需求指的是用户对 CPS 的需求, 是用户建立 CPS 的目的. 该活动的任务就是与用户进行沟通, 获取用户对将要建立的 CPS 的需求陈述.

其次, 推理软件需求. 该步骤的任务是由用户需求出发, 采取面向目标的策略来推理分析软件需求. 在此过程中, 一方面, 分析人员需要权衡满足用户需求的方案, 选择构成系统的不同物理实体和软件实体, 分析物理实体的性质和软件实体的需求; 另一方面, 分析人员需要逐步建立系统的结构模型和目标模型来描述分析的结果.

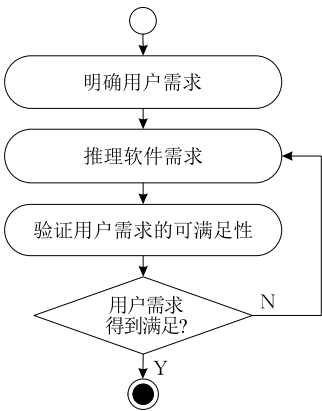


图 4 本文方法的基本过程

第三, 验证用户需求的可满足性. 该步骤基于上述两步的分析结果, 利用 Alloy 来描述所识别的物理实体的性质和软件实体的需求, 进而验证基于所描述的物理性质和软件需求用户需求是否能够得到满足, 并在用户需求不能满足时, 返回第二步, 改进所建立的模型.

本文将在第 4 节以 2.1 节所描述的自适应巡航控制系统为例, 逐步详细介绍该过程.

4 方法说明

以自适应巡航控制系统为例, 本节执行图 4 所示的需求分析过程, 并详细说明该过程每步活动所采取的具体策略.

(1) 明确用户需求

用户需求是用户对 CPS 的需求. 基于问题框架方法, 用户对 CPS 的需求存在于 CPS 的运行环境之中, 表达的是希望当某些现象发生时使得另外一些现象的发生, 即 CPS 要实现的是一种现象之间的因果关系. 因此, 本文采用现象间的因果关系表达式来明确地描述用户的需求. 以自适应巡航控制系统为例, 其用户需求可以表达为如下的一组现象间的因果关式:

$$R = \{r_1, r_2, r_3, r_4\}.$$

$r_1 = p_1$: 前方没有车 $\wedge$ p_2 : 被控车辆速度不大于巡航速度 $\rightarrow p_3$: 被控车辆加速到巡航速度

$r_2 = p_1$: 前方没有车 $\wedge$ p_4 : 被控车辆速度大于巡航速度 $\rightarrow p_5$: 被控车辆减速到巡航速度

$r_3 = p_6$: 前方有车 $\wedge$ p_7 : 两车间距不大于安全距离 $\rightarrow p_8$: 增大间距使得两车间距等于安全距离

$r_4 = p_6$: 前方有车 $\wedge$ p_9 : 两车间距大于安全距离 $\rightarrow p_{10}$: 减少间距使得两车间距等于安全距离

在上述的现象因果关式式中, 箭头前端的现象为用户需求所引用的可观测现象, 如 p_1, p_6 ; 箭头后端的现象为用户需求所引用的可控现象, 也即目标现象, 如 p_3, p_5 . 为了进一步帮助分析人和用户进行有效的沟通, 本文引用图 1 所示的问题图的部分元素, 定义了图 5 所示的用户需求框图, 来展现用户在描述需求时其语境中所涉及到的实体(一般是物理实体)以及所引用的实体现象.

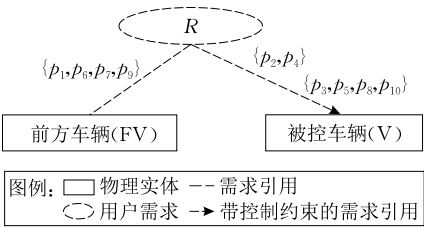


图 5 用户需求框图

实际中, 分析人员在明确用户需求的过程中不仅需要分析用户需求所引用的物理实体和现象, 还要判断用户需求因果关式式中箭头前端所引用的现

象是否是可观测的,箭头后端所引用的现象是否是可控的.否则,分析人员就需要与用户沟通,通过进一步分析用户问题来厘清用户对 CPS 的需求.

(2) 推理软件需求

通过将用户需求表达为现象间的因果关系式,我们确定了一组可观测现象和可控现象.那么,进一步分析软件需求的目的就是建立可观测现象到可控现象的因果关系链(如 p_1 和 p_2 到 p_3 的因果关系链)、识别该因果关系链中所涉及的实体以及实体之间的共享现象(因果关系链中可观测现象到可控现象之间的中间现象).

为实现这一目的,本文方法的基本思路是采用图 2 所示的目标模型,将目标模型中的目标、领域假设、任务表达为现象之间的因果关系(认为这些概念表达的也是现象之间的因果关系),然后将用户需求的因果关系式作为目标模型中的“目标”,进而通过将“目标”分解为“领域假设”和“任务”来分析满足用户需求的因果关系链的不同片段.其中“领域假设”的因果关系刻画的是物理实体所具有的性质,“任务”所描述的因果关系刻画的是软件实体所应实现的需求.

在具体的目标分解过程中,本文方法采取如下两种分解策略:

① 问题转换.通过引入部分解决方案来将一个目标转换为另外一个问题,使得原始问题更小、更容易解决^[6];

② 问题分解.将一个问题分解为一组子问题,这些子问题解决方案的组合就是原始问题的解决方案,降低原始问题的复杂性^[7].

问题转换和问题分解是问题框架方法中分解问题的两种方式.为了应用这两种方式,本文方法将每个目标(也即一个现象间因果关系式)看作一个问题.具体的应用方式如下:

问题转换意味着将一个目标分解为多个领域假设和其他目标.这些领域假设描述的是一个或者多个物理实体的输入现象到输出现象的因果关系,体现这些物理实体的性质,并且该因果关系的输入现象或者输出现象能够匹配目标因果关系式中的现象.在这种情况下,这些物理实体可以作为构成 CPS 的一部分(部分解决方案),其输入现象到输出现象的因果关系也成为满足目标因果关系链的一部分.

问题分解则意味着将一个目标分解为一个或多

个其他目标或者任务.这一般发生于分析人员已知满足一个目标的完整或者部分过程.此时,他可以将该过程分解为不同的步骤,然后定义不同步骤之间的共享现象.此时每步的输入现象和输出现象之间的因果关系可以表达为目标模型中的一个任务(如果实现该因果关系可以作为一个任务分配给一个软件实体)或者一个新目标(如果实现该因果关系不能作为一个任务分配给一个软件实体,则将其作为一个新目标继续进行分解).

自适应巡航控制系统的用户需求包含了四组因果关系式.以第一组因果关系式($p_1 \wedge p_2 \rightarrow p_3$)为例,图 6 所示的目标模型展示了应用问题转换和问题分解的软件需求分析过程,图 7 呈现的是记录该分析过程所识别的实体及其之间关系的结构模型.如图 6 所示,为了突出该基于目标的分析过程中所涉及的各个实体,本文方法在每个因果关系式前面标明实现该因果关系式的实体(例如, $T(R: p_1 \rightarrow p'_1)$ 中 R 表明实现因果关系 $p_1 \rightarrow p'_1$ 的实体是雷达 R ,如果实现该因果关系式的实体还未明确,则显示为“?”).如图 7 所示,本文应用了图 1 所示的问题图来表示结构模型.不同的是该结构模型以箭头的方向来表示共享现象的控制方向,以领域实体的符号来表示物理实体,并且一个问题图中可以有多个软件实体,每个实体还可以继续分解(如图 9 所示).本文对该分析过程的解释如下.

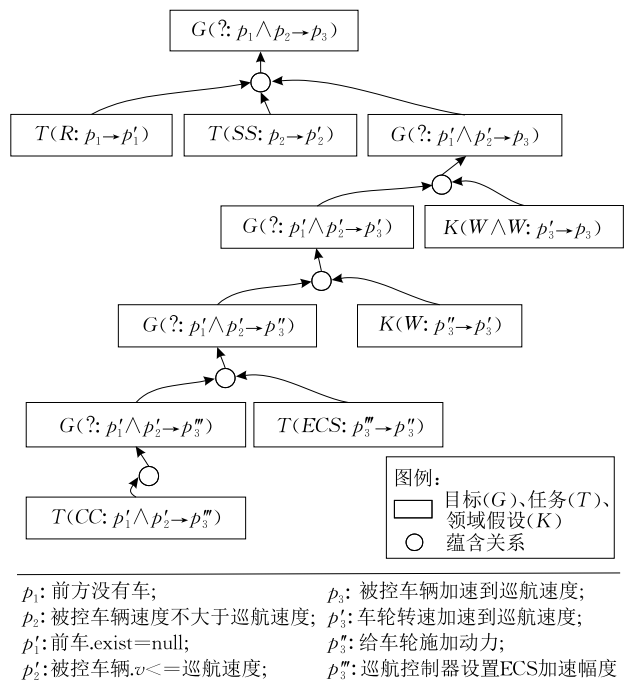


图 6 基于目标的软件需求的分析过程

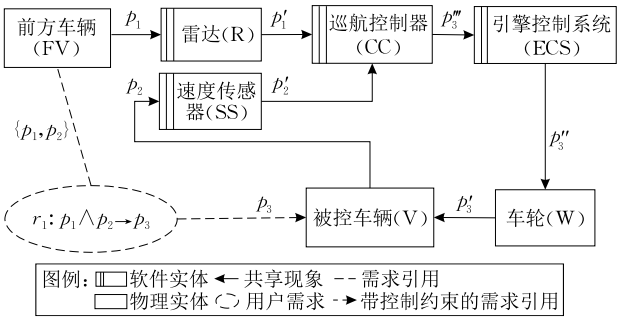


图 7 以问题图所表示的结构模型

首先,从 $p_1 \wedge p_2 \rightarrow p_3$ 的可观测现象 p_1 和 p_2 出发,如果要想实现当前方没有车(p_1)和被控车辆的速度不大于巡航速度(p_2)时控制被控车辆的速度达到巡航速度(p_3),必须首先感知到 p_1 和 p_2 的发生,然后才能做出响应来控制被控车辆的速度.这里感知到 p_1 和 p_2 的发生即是我们已知的实现该因果关系的部分过程,而感知 p_1 可以通过设计开发一个雷达来实现,雷达将该现象转换为由雷达测量值所表达的现象 p'_1 (前车.exist=null),感知 p_2 则可以通过设计开发一个测速传感器来实现,测速传感器将该现象转换为由具体的车速值所表达的事件 p'_2 (被控车辆.v≤巡航速度).这里的雷达和测速传感器是我们通过分析所识别的两个软件实体(虽然实际中雷达和测速传感器可直接购买而不需要设计开发,但从设计的角度出发,本文把它们作为需要设计开发的软件实体).从现象 p_1 到 p'_1 和从现象 p_2 到 p'_2 的因果关系分别体现了雷达和测速传感器应实现的需求.由于实现这两个因果关系的实体已知(雷达和测速传感器),该因果关系也因此可以表达为目标模型中关于软件实体雷达和测速传感器的任务: $T(R: p_1 \rightarrow p'_1)$ 和 $T(SS: p_2 \rightarrow p'_2)$.如图 6 所示,基于这两个任务,目标 $G(? : p_1 \wedge p_2 \rightarrow p_3)$ 通过问题分解可以转化为目标 $G(? : p'_1 \wedge p'_2 \rightarrow p_3)$.

其次,由于汽车的速度等于车轮的转速,可以通过触发现象 p'_3 来实现目标现象 p_3 的触发,即通过将车轮的转速加速到巡航速度来实现被控车辆的速度达到巡航速度.因此,基于问题转换,可以将从 p'_3 到 p_3 的因果关系表达为领域假设 $K(W \wedge V: p'_3 \rightarrow p_3)$ 来体现汽车和车轮之间关系所具有的性质,并且基于该领域假设目标 $G(? : p'_1 \wedge p'_2 \rightarrow p_3)$ 可以转化为目标 $G(? : p'_1 \wedge p'_2 \rightarrow p'_3)$.

更进一步,由于控制车轮的转速加速到巡航速度可以通过给车轮施加相应的动力来实现,现象 p'_3

的触发可以通过触发 p'_3 来实现.从 p'_3 到 p'_3 之间的因果关系体现了车轮这一物理实体的性质.因此,基于问题转换,将从 p'_3 到 p'_3 之间的因果关系表达为目标模型中关于车轮这一物理实体的领域假设 $K(W: p'_3 \rightarrow p'_3)$,并基于该假设,目标 $G(? : p'_1 \wedge p'_2 \rightarrow p'_3)$ 可以继续转化为目标 $G(? : p'_1 \wedge p'_2 \rightarrow p''_3)$.

最后,由于已知可以设计开发一个 ECS(引擎控制系统)来对车轮施加动力,ECS 可以根据设定的加速幅度指令(p''_3)来给车轮施加相应的动力(p'_3),从 p''_3 到 p'_3 的因果关系体现对 ECS 这一软件实体的需求.因此,基于问题分解,将 p''_3 到 p'_3 的因果关系表达为关于 ECS 的任务: $T(ECS: p''_3 \rightarrow p'_3)$, $G(? : p'_1 \wedge p'_2 \rightarrow p'_3)$ 可以转化为目标 $G(? : p'_1 \wedge p'_2 \rightarrow p''_3)$.而由于 $G(? : p'_1 \wedge p'_2 \rightarrow p''_3)$ 这一目标可以完全赋给一个新的软件实体“巡航控制器(CC)”来实现,因此该目标可以转化为任务 $T(CC: p'_1 \wedge p'_2 \rightarrow p''_3)$.

至此,如图 7 所示,上述过程分析了实现 $p_1 \wedge p_2 \rightarrow p_3$ 这一因果关系所需要物理实体、软件实体以及它们之间的共享现象.并且,由 $p_1, p_2, p'_1, p'_2, p''_3, p'_3, p_3$ 所构成的现象间因果关系链条体现了满足 $r_1(p_1 \wedge p_2 \rightarrow p_3)$ 这一用户需求的计算过程与物理过程的融合.图 6 中所展示的领域假设体现了物理实体的性质,任务体现了软件实体应满足的需求.

实际中,当如图 6 所示的目标模型的所有叶节点都为领域假设和任务时,针对一个目标的分解过程终止.并且,分析人员针对用户需求中的每个因果关系表达式,遵循上述分析过程就可以得出每个因果关式对应的目标模型(如图 6 所示)和结构模型(如图 7 所示),然后合并每个结构模型,就可以得到反映 CPS 的构成实体及其实体间关系的完整结构模型(本文这里为减少篇幅省略了对 r_2, r_3, r_4 分析过程的介绍).

对于上述分析过程所形成的有些领域假设和任务(图 6 目标模型的叶节点),可以将其当作一个新的目标,然后应用上述的分析策略来进行进一步的分解.一个领域假设可以分解为其他的领域假设;一个任务可以分解为更具体的任务.但是,如果在继续分解的过程中出现了新的实体,那么该领域假设或者任务的分解过程则对应着相应的物理实体或者软件实体结构上的分解.例如,图 8 展示了任务 $T(ECS: p''_3 \rightarrow p'_3)$ 的分解过程(将该任务当作新的目标 $G(ECS: p''_3 \rightarrow p'_3)$),图 9 是对引擎控制系统(ECS)这一软件实体进行分解的相应结果.

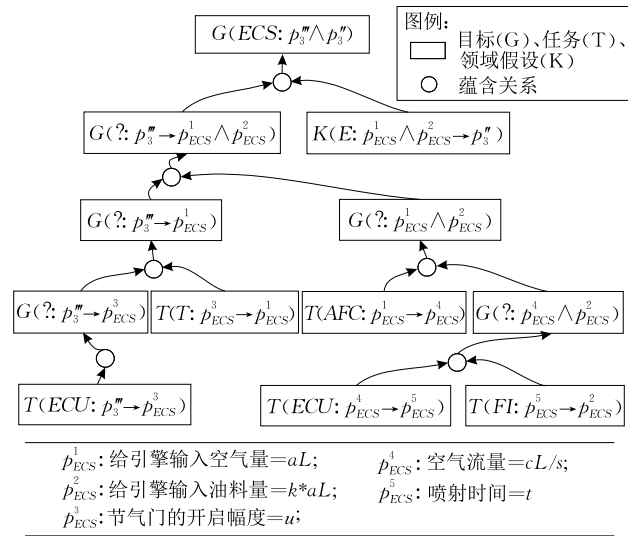


图 8 对任务 $T(ECS: p_3''' \rightarrow p_3'')$ 进一步分解的目标模型

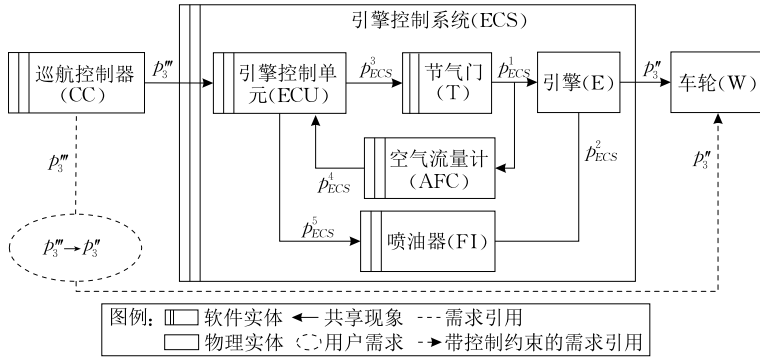


图 9 对任务 $T(ECS: p_3''' \rightarrow p_3'')$ 进一步分解所得到的刻画 ECS 结构的结构模型

者性质,用户的需求是否可以得到满足.

本文基于 Alloy 来实现这一目的. Alloy 是一种轻量级的面向对象的描述语言,使用 signature 来表示一个类型,代表具有某类特征的对象集合.在定义一个 signature 时不仅可以通过定义 field 来描述与当前数据类型存在关系的其他类型,还可以定义该类型对象所遵循的约束.同时,分析人员也可以通过定义 fact 来描述类型之间的关系.而需要验证的事实或者结论则可以通过定义断言 assert 来描述.最后,分析人员可以利用 Alloy 分析器来验证断言的真假.

本文将所识别的构成 CPS 的每个实体定义为一个 signature,将实体所具有的一些现象定义为 signature 的 field,并将实体具有的性质或者应满足的需求(现象间的因果关系)定义为 signature 的约束(通过 imply 关系来描述现象间的因果关系式),然后通过定义不同的 assert 来描述用户需求中的不同因果关系式.以自适应巡航控制系统为例,图 10 展示了对物理实体“车轮(W)”和软件实体“引擎控

制系统(ECS),其输出的动力跟输入引擎的油气量有关,而往往为了追求最大的燃油效率,输入的空气量和油量成比例,因此目标 $G(ECS: p_3''' \rightarrow p_3'')$ 可以分解为目标 $G(? : p_3''' \rightarrow p_{ECS}^1 \wedge p_{ECS}^2)$ 和关于引擎这一物理实体的领域假设 $K(p_{ECS}^1 \wedge p_{ECS}^2 \rightarrow p_3'')$,并且目标 $G(? : p_3''' \rightarrow p_{ECS}^1 \wedge p_{ECS}^2)$ 可以进一步分解为目标 $G(? : p_3''' \rightarrow p_{ECS}^1)$ 和目标 $G(? : p_{ECS}^1 \rightarrow p_{ECS}^2)$,其中 $G(? : p_{ECS}^1 \rightarrow p_{ECS}^2)$ 表达的是根据输入的空气量来给引擎输入相应的比例的油量.

(3) 验证用户需求的可满足性

经过前面两步的分析,我们可以得到满足用户需求的一组物理实体、软件实体以及通过现象因果关系式所表达的实体需求或者性质.在这种情况下,第三步活动的目的就是验证基于这些实体的需求或

制系统(ECS)”的定义.图 11 显示了通过断言来描述的自适应巡航控制系统的用户需求.

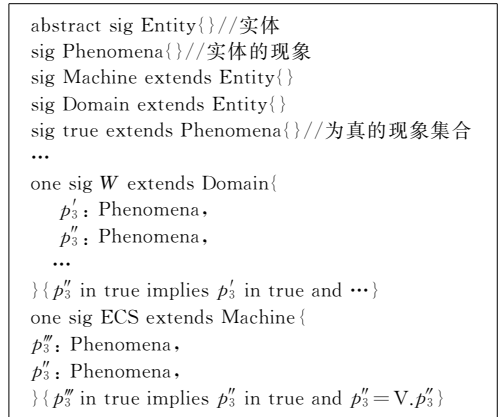


图 10 “车轮”和“引擎控制系统”的 Alloy 描述

如图 10 所示,对于车轮而言,它定义中第 1 个大括号内的 p_3' 和 p_3'' 是描述其物理性质的因果关系式中的现象(见图 6 和图 7);第 2 个大括号内的表达式是对体现其性质的现象因果关系的描述.而对于软件实体引擎控制系统,其第 1 个大括号同样是

对其相关现象的描述,第 2 个大括号内的表达式则是对其实实现的现象因果关系的描述. 并且实体间的某些现象是共享的这一事实也可以在实体定义中的第 2 个大括号内描述(如图 10 中 ECS 的第 2 个大括号内 $p_3''=V.p_3''$).

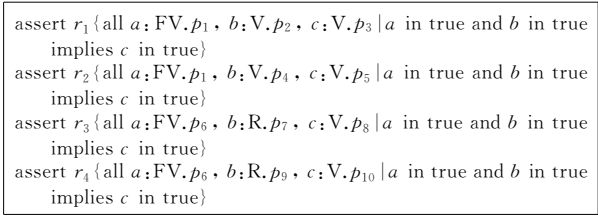


图 11 自适应巡航控制系统用户需求的 Alloy 描述

5 相关工作

CPS 在过去几年里得到了大量的关注. 而 CPS 的需求分析与建模作为 CPS 研究领域中的一个重要问题,也吸引着许多研究人员去探讨面临的挑战和研究具体的方法.

在面临的挑战方面,Derler 等人^[8]介绍了在建模过程中所面临的困难以及可用的相关技术;Wan 等人^[9]讨论了在 CPS 的需求描述和分析方面的挑战;Wang 等人^[10]阐述了在 CPS 安全性方面潜在的问题和挑战;而 Banerjee 和 Gupta 则指出在控制系统和混合系统中通常使用的解决方案并不适用于 CPS 的分析和建模,因为它们依赖的假设对于 CPS 是不成立的^[11].

在具体方法方面, Ringert 等人^[12]提出结合 ADL 和 I/O 自动机来描述 CPS,以利用 ADL 来建模 CPS 的结构、利用 I/O 自动机来描述构成 CPS 的各个组成部分的行为;Henriksson 和 Elmqvist^[13]认为 Modelica 语言适用于 CPS 的需求建模和仿真;Bujorianu 等人^[14-15]基于 Hilbertean 提出一个统一的逻辑语言来描述 CPS;朱敏等人^[16]提出基于微分动态逻辑来描述 CPS 的需求和进行属性验证;Banerjee 和 Gupta^[17]提出采用混合自动机来建模信息物理医疗系统;周兴社等人^[18]提出基于 CPS-ADL 来对 CPS 系统动态行为模型进行构建;尹玲等人^[19]则提出了一个基于逻辑时钟的 CPS 时间需求一致性分析框架;针对交通 CPS,Zhang^[20]通过扩展 AADL 来表达交通 CPS 的行为性质、动态连续特征和时空需求;针对汽车 CPS,Zhang^[21]进一步综合 AADL、Modelica、UML 等来描述汽车 CPS 的需

求,其中利用 AADL 和 UML 来描述汽车 CPS 的软件部分,利用 Modelica 来描述物理部分,最后提出通过形式化方法来检验所建立的需求模型是满足系统功能、性能等需求;更进一步,Zhang^[22]还基于 AADL 来描述 CPS QoS 方面的需求.

从面向服务的角度出发,国外的 Huang 等人^[23]和国内的李戈等人^[24]均提出扩展现有的服务模型来为 CPS 的建模提供解决方案. 除此之外,Murugesan 等人在文献^[25]中提出了一个方法来建立系统的早期结构模型,以帮助确定系统的范围,在该结构模型中,系统的组成部分通过其输入和输出来描述.

上述关于 CPS 需求分析和建模方面的工作侧重于 CPS 需求的建模,主要关注于如何描述和验证 CPS 的结构或者行为. 不同于这些工作,本文侧重于 CPS 的需求分析,主要关注于如何来厘清用户需求,如何从用户需求出发去分析系统所要涉及的软件实体、物理实体、它们的性质和行为等.

作为 CPS 的重要组成部分,CPS 的物理实体处于连续世界,因此 Heimdahl 等人认为对于 CPS 的物理实体,我们不仅需要分析实时性需求,还要分析其连续性质方面的需求. 对此,受阶跃信号的不同物理性质启发,Heimdahl 等人^[26]提出了 6 种对物理实体的需求. 对于物理实体的需求,本文仅分析了物理实体功能性方面的性质,对于时间以及连续性方面的性质目前还没有涉及,这是我们未来考虑 CPS 非功能性需求时的研究工作.

而在将软件需求工程的问题框架方法和面向目标的方法结合起来,以充分借鉴不同方法的优点方面,Liu 和 Jin^[27]曾将面向目标的 i* 方法与问题框架方法结合以提高 i* 的表达能力;而 Mohammadi 等人在文献^[28]中提出了一个框架来融合面向目标的方法、问题框架方法以及序列图以弥补面向目标方法和问题框架方法的各自缺点. 不同于上述工作,本文的主要目的是融合问题框架方法和面向目标方法来推理分析构成 CPS 的软件实体、物理实体和它们的性质而不是改进二者的缺点,因此本文两种方法的融合过程都是从 CPS 的具体特点出发,比如将问题框架方法的问题转换和分解策略用来指导目标分解.

6 结束语

本文提出了一种分析 CPS 软件需求的方法. 它

有助于分析人员从用户对 CPS 的需求出发,分析满足用户需求所需要的物理实体、软件实体以及物理实体的性质和软件实体的需求,并验证这些实体所构成的 CPS 是否能够满足用户的需求. 本文通过一个自适应的巡航控制系统说明了该方法的可行性.

本文以现象间的因果关系式这一形式来描述用户需求,该方式能够呈现用户需求的具体结构,即用户期望的是在哪些现象发生的情况下触发另外哪些现象的发生. 但是,在实际中用户所引用的现象可能比较复杂,比如用户期望在现象 a 发生,现象 b 不发生的情况下发生现象 c . 对于如何处理这一细节,本文目前还没涉及. 还有,用户需求集合中的不同需求对应着不同的现象因果关系链(如第 4 节所示),而这些现象因果关系链在实际的执行过程中可能存在着冲突,比如共享某些现象或者实体. 如何检测和解决这些潜在的冲突本文目前还没有考虑. 另外,计算过程和物理过程的融合使得时间和空间特征(现象的时间和空间属性)成为 CPS 软件分析过程中所必须考虑的问题,对此本文方法目前也没有涉及. 因此,在未来的工作中我们将就上述方面进行进一步的研究.

参 考 文 献

- [1] Lee E A. Cyber-physical systems-are computing foundations adequate//Proceedings of the NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap. Austin, USA, 2006
- [2] Wen Jing-Rong, Wu Mu-Qing, Su Jing-Fang. Cyber-physical system. *Acta Automatica Sinica*, 2012, 38(4): 507-517 (in Chinese)
(温景荣, 武穆清, 宿景芳. 信息物理融合系统. 自动化学报, 2012, 38(4): 507-517)
- [3] Jackson M. Problem Frames: Analyzing and Structuring Software Development Problems. Boston, USA: Addison-Wesley, 2001
- [4] Jureta I J, Borgida A, Ernst N A, et al. The requirements problem for adaptive systems. *ACM Transactions on Management Information Systems*, 2014, 5(3): 17
- [5] Jackson D. Alloy: A lightweight object modeling notation. *ACM Transactions on Software Engineering and Methodology*, 2002, 11(2): 256-290
- [6] Seater R, Jackson D, Gheyi R. Requirement progression in problem frames: Deriving specifications from requirements. *Requirements Engineering*, 2007, 12(2): 77-102
- [7] Hall J G, Rapanotti L, Jackson M A. Problem oriented software engineering: Solving the package router control problem. *IEEE Transactions on Software Engineering*, 2008, 34(2): 226-241
- [8] Derler P, Lee E A, Vincentelli A S. Modeling cyber—physical systems. *Proceedings of the IEEE*, 2012, 100(1): 13-28
- [9] Wan K, Man K L, Hughes D. Specification, analyzing challenges and approaches for cyber-physical systems (CPS). *Engineering Letters*, 2010, 18(3): 308
- [10] Wang E K, Ye Y, Xu X, et al. Security issues and challenges for cyber physical system//Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International Conference on Cyber, Physical and Social Computing. Chengdu, China, 2010: 733-738
- [11] Banerjee A, Gupta S K S. Tackling new frontiers in modeling and analysis of cyber-physical systems//Proceedings of the 1st Workshop on Cyber-Physical Systems Education. Philadelphia, USA, 2013: 1-4
- [12] Ringert J O, Rumpe B, Wortmann A. A requirements modeling language for the component behavior of cyber physical robotics systems//Seyff N, Koziolok A eds. *Modelling and Quality in Requirements Engineering: Essays Dedicated to Martin Glinz on the Occasion of His 60th Birthday*. Münster: Monsenstein und Vannerdat, 2012: 143-155
- [13] Henriksson D, Elmqvist H. Cyber-physical systems modeling and simulation with Modelica//Proceedings of the 8th International Modelica Conference. Dresden, Germany, 2011: 502-509
- [14] Bujorianu M C, Barringer H. An integrated specification logic for cyber-physical systems//Proceedings of the 14th IEEE International Conference on Engineering of Complex Computer Systems. Potsdam, Germany, 2009: 291-300
- [15] Bujorianu M C, Bujorianu M L, Barringer H. A unifying specification logic for cyber-physical systems//Proceedings of the 17th Mediterranean Conference on Control and Automation. Thessaloniki, Greece, 2009: 1166-1171
- [16] Zhu Min, Li Bi-Xin, Chen Qiao-Qiao, et al. Transforming hybrid UML to hybrid program for CPS property verification. *Acta Electronica Sinica*, 2012, 40(6): 1126-1132 (in Chinese)
(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. 电子学报, 2012, 40(6): 1126-1132)
- [17] Banerjee A, Gupta S K S, Fainekos G, et al. Towards modeling and analysis of cyber-physical medical systems//Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. Barcelona, Spain, 2011: 154
- [18] Zhou Xing-She, Yang Ya-Lei, Yang Gang. Modeling methods for dynamic behaviors of cyber-physical system. *Chinese Journal of Computers*, 2014, 37(6): 1411-1423 (in Chinese)
(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. 计算机学报, 2014, 37(6): 1411-1423)
- [19] Yin Ling, Chen Xiao-Hong, Liu Jing. Consistency analysis of timing requirements for cyber-physical system. *Journal of Software*, 2014, 25(2): 400-418 (in Chinese)

(尹玲, 陈小红, 刘静. 信息物理融合系统的时间需求一致性分析. 软件学报, 2014, 25(2): 400-418)

- [20] Zhang L C. Requirement specification for transportation cyber physical systems//Proceedings of the 2013 IEEE International Conference on Green Computing and Communications. Beijing, China, 2013: 1486-1491
- [21] Zhang L C. Specifying and modeling automotive cyber physical systems//Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering. Sydney, Australia, 2013: 603-610
- [22] Zhang L C. Specification and modeling of QoS based on AADL //Proceedings of the 5th IEEE International Conference on Software Engineering and Service Science. Beijing, China, 2014: 1107-1110
- [23] Huang J, Bastani F, Yen I L, et al. Extending service model to build an effective service composition framework for cyber-physical systems//Proceedings of the 2009 IEEE International Conference on Service-Oriented Computing and Applications (SOCA). Taipei, China, 2009: 1-8
- [24] Li Ge, Wei Qiang, Li Li-Xing, et al. The modeling of services in the Internet of Things: A method based on environmental modeling. Scientia Sinica Informations, 2013, 43(10): 1198-

1218(in Chinese)

(李戈, 魏强, 李力行等. 物联网服务建模: 一种基于环境建模的方法. 中国科学: 信息科学, 2013, 43(10): 1198-1218)

- [25] Murugesan A, Rayadurgam S, Heimdahl M. Using models to address challenges in specifying requirements for medical cyber-physical systems//Proceedings of the 4th Workshop on Medical Cyber-Physical Systems. Philadelphia, USA, 2013
- [26] Heimdahl M P E, Duan L, Murugesan A, et al. Modeling and requirements on the physical side of cyber-physical systems//Proceedings of the 2nd International Workshop on the Twin Peaks of Requirements and Architecture (Twin-Peaks). San Francisco, USA, 2013: 1-7
- [27] Liu L, Jin Z. Integrating goals and problem frames in requirements analysis//Proceedings of the 14th IEEE International Requirements Engineering Conference (RE'06). St. Paul, USA, 2006: 349-350
- [28] Mohammadi N G, Alebrahim A, Weyer T, et al. A framework for combining problem frames and goal models to support context analysis during requirements engineering//Availability, Reliability, and Security in Information Systems and HCI. Berlin: Springer, 2013: 272-288



LIU Chun, born in 1982, Ph. D., lecturer. His main research interest focuses on requirements engineering.

HUANG Ran-Ran, born in 1989, M. S. candidate. Her main research interest focuses on requirements engineering.

ZHANG Wei, born in 1978, Ph. D., associate professor.

His main research interests include software requirements engineering and software reusability.

ZHAO Hai-Yan, born in 1966, Ph. D., associate professor. Her main research interests include software engineering and domain engineering.

JIN Zhi, born in 1962, Ph. D., professor, Ph. D. supervisor. Her main research interests include requirements engineering, knowledge engineering and knowledge-based software engineering.

Background

This paper focuses on the issue of how to analyze the software requirements of cyber-physical systems (CPS), i. e., how to identify the software entities in CPS and derive their requirements from the users' requirements on CPS. It is part of the work on requirements analysis and modeling of CPS. By now there is already a lot of work addressing how to model CPS, however, there still lacks of effective approaches to analyze the software requirements in CPS. This paper proposes such an approach which currently can derive functional requirements of the software entities in cyber-physical systems. And in the future, we will improve it with the ability to

analyze the non-functional requirements.

The work of this paper belongs to our research project on requirements analysis and modeling of CPS supported by the China Postdoctoral Science Foundation (No. 2014M552000), the Key Laboratory of High Confidence Software Technologies of Ministry of Education (No. HCST201301) and the Foundation of Henan Educational Committee (No. 14A520009). This project aims to design an approach to help analysts acquire users' requirements on CPS, derive software requirements from users' requirements, and finally model these requirements and validate the satisfaction of users' requirements.