我们在为一家互联网电商开发订单处理软件，该公司从供应商那里购买产品，然后销售给客户。这家公司在线发布商品目录，并将其推送给客户和其他感兴趣的人。

客户以提交商品列表并向电商付费的方式购买商品。电商填写帐单，并委托快递公司把商品运送到客户的地址。订单处理软件记录从收到订单直到商品被运送给客户的整个过程。电商将提供快捷的服务，以最快、最有效的方法来发送客户订购的产品。
客户可以退货，但有时要付运费。

单选题 1分

进入订购商品用例的前置条件是:

A 客户对商品感兴趣

B 客户安装了与系统兼容的浏览器版本

C 商品已经放入购物车

D 客户通过合法账户登入系统

单选题 1分

使用订单处理系统一段时间以后，电商希望增加一种功能——为老顾客提供折扣。以下哪种方法比较合适？

A 建立老顾客折扣新用例

B 扩展订购商品用例

C 在订购商品用例中包含老顾客提供折扣用例

D 为订购商品用例建立两个子用例：普通顾客订购商品和老顾客订购商品

基于环境建模的方法

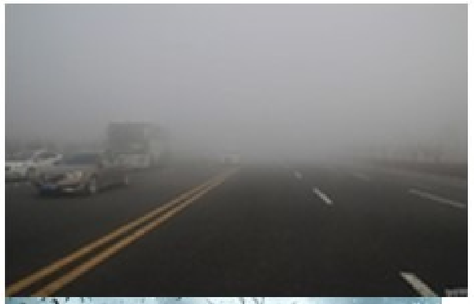
徐思涵

南开大学

Slides adapted from materials by Prof. Qiang Liu (Tsing Hua University) and Ivan Marsic (Rugers University)

案例

自动驾驶系统能在没有用户干预的情况下,自动规划行车路线并控制车辆行驶。控制软件是自动驾驶系统的核心部件,它可以调度各种车载传感器,感知车辆所处的道路环境,并根据当前道路状况、车辆位置以及是否有障碍物等,实时进行行为决策,控制车辆的行进、转向和速度等,使车辆安全行驶到达目的地。



概述

基于环境建模的需求工程以系统环境模型为基础,

- 帮助需求工程师识别系统的环境关注点,
- 引导其对这些环境关注点进行系统化的分析,
- 从中引导出系统和环境的交互能力需求。

假设环境模型承载了待开发系统需要掌握的环境知识,在进行系统需求建模和分析时,可以从环境知识和用户需求出发,推断并规约系统需求。

概述

软件需求工程的本质：

$$E, S \models R$$

- E通常假设运行在相对静态、封闭和确定的环境
- 但像自动驾驶这类系统,它们将运行在开放、动态的交互环境中
- 需求阶段不能假设系统环境的特征能事先完全确定,系统行为能力需求来自可能的环境实体的行为。

- 环境模型：
  - 支撑这类软件系统的需求获取和规约，
  - 还可以用于指导这类系统的需求验证等

环境建模和环境本体

基于环境建模的方法将环境实体作为第一类概念

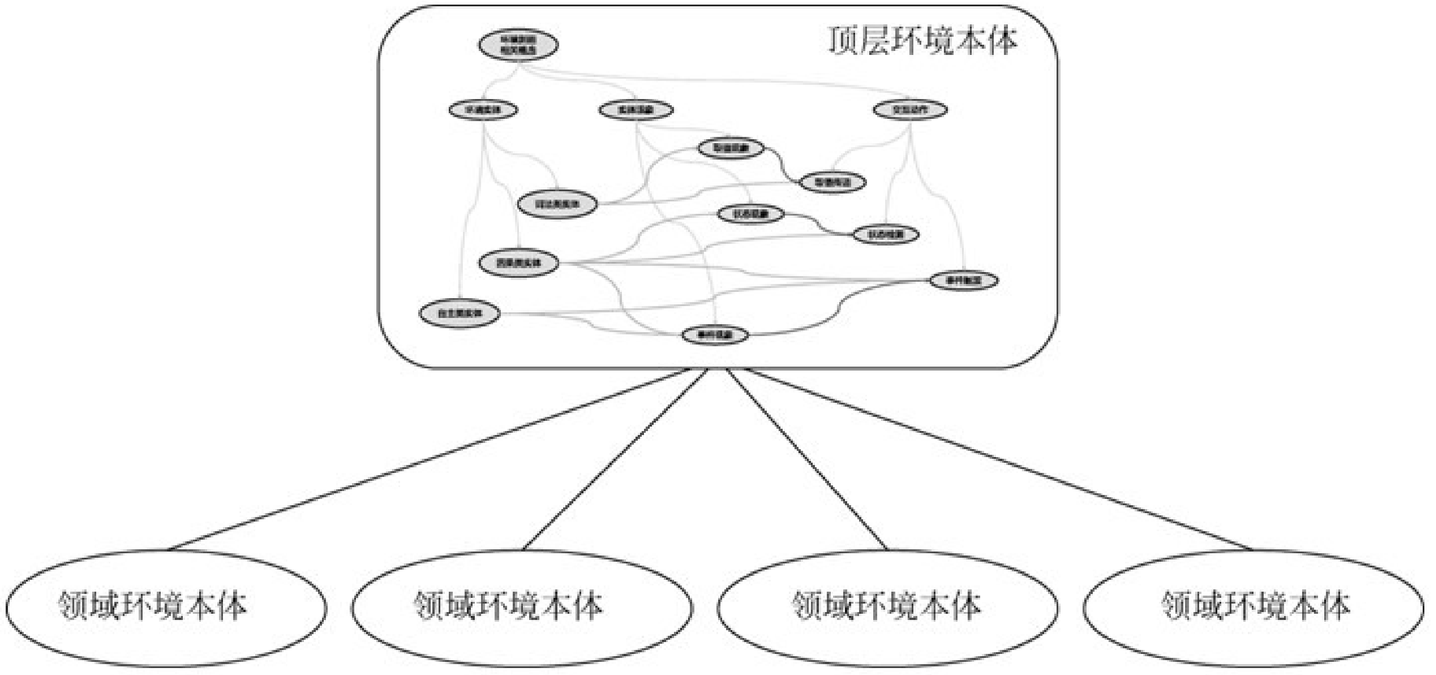
概念抽象原则：

- **建模原则一(环境实体的类型化)：** 根据环境实体的属性或特征，对环境实体进行类型化，分门别类进行建模。
- **建模原则二(环境实体的状态化)：** 一些环境实体在不同情况下会具有不同特征，据此抽象出环境实体的内部状态。环境实体在不同时刻处于不同状态。
- **建模原则三(环境实体的因果性)：** 具有内部状态的环境实体会展现出自身遵循的行为规律，即呈现其内在的行为因果性。

环境建模和环境本体

环境本体

- 顶层环境本体包括环境模型的通用概念、通用概念关联及其相关约束
- 领域环境本体包括特定应用领域的环境相关概念、关联和约束
- 领域环境本体是顶层环境本体在特定领域的实例化



环境本体的层次

顶层环境本体

1．环境本体的概念和关联

环境实体(Environment Entity)：

- 因果类实体(Causal Entity，C为其类型标记)

主要指问题驱动方法的因果领域，表示一类物理存在的实体，**主要刻画其因果性特征，即内部存在明确的具有因果关系的行为规律，可以假设在与它相关的交互现象之间存在可预测的因果关系。**

- 自主类实体(Autonomous Entity，A为其类型标记)

基本涵盖问题驱动方法的顺从式领域，**表示一类物理存在的实体**，但与因果类实体不同的是，这类实体假设是自治的，没有明确的(或者目前还不清楚其)内部因果性，**不能假设与它相关的交互现象存在确定可预测的因果关系。**

- 符号类实体(Symbolic Entity，S为其类型标记)

继承问题驱动方法中的词法领域，一般是设计出来的**数据**或者是**信息的物理存储。**

顶层环境本体

1. 环境本体的概念和关联

顶层概念的含义

概念类别	概　　念	概 念 含 义
环境实体	符号类实体	一般是设计出来的数据或其他信息的物理存储
	自主类实体	自治的物理存在的实体，没有明确的内部因果性，不能假设与它相关的交互现象之间存在确定的因果关系。
	因果类实体	物理存在的实体，特征是其内部存在明确的具有因果关系的行为规律，可以假设在与它相关的交互现象之间存在可预测的因果关系
个体现象	取值现象	某个属性在某一时刻所取的特定的值
	状态现象	因果类实体在某一时刻所处的特定的情况
	事件现象	某个特定时间点上发生或者出现的事情或事项，被看作原子的和瞬间的
实体交互	取值传递	“属性-取值”对
	状态检测	“实体-状态”对
	事件触发	“实体-事件”对

顶层环境本体

1. 环境本体的概念和关联

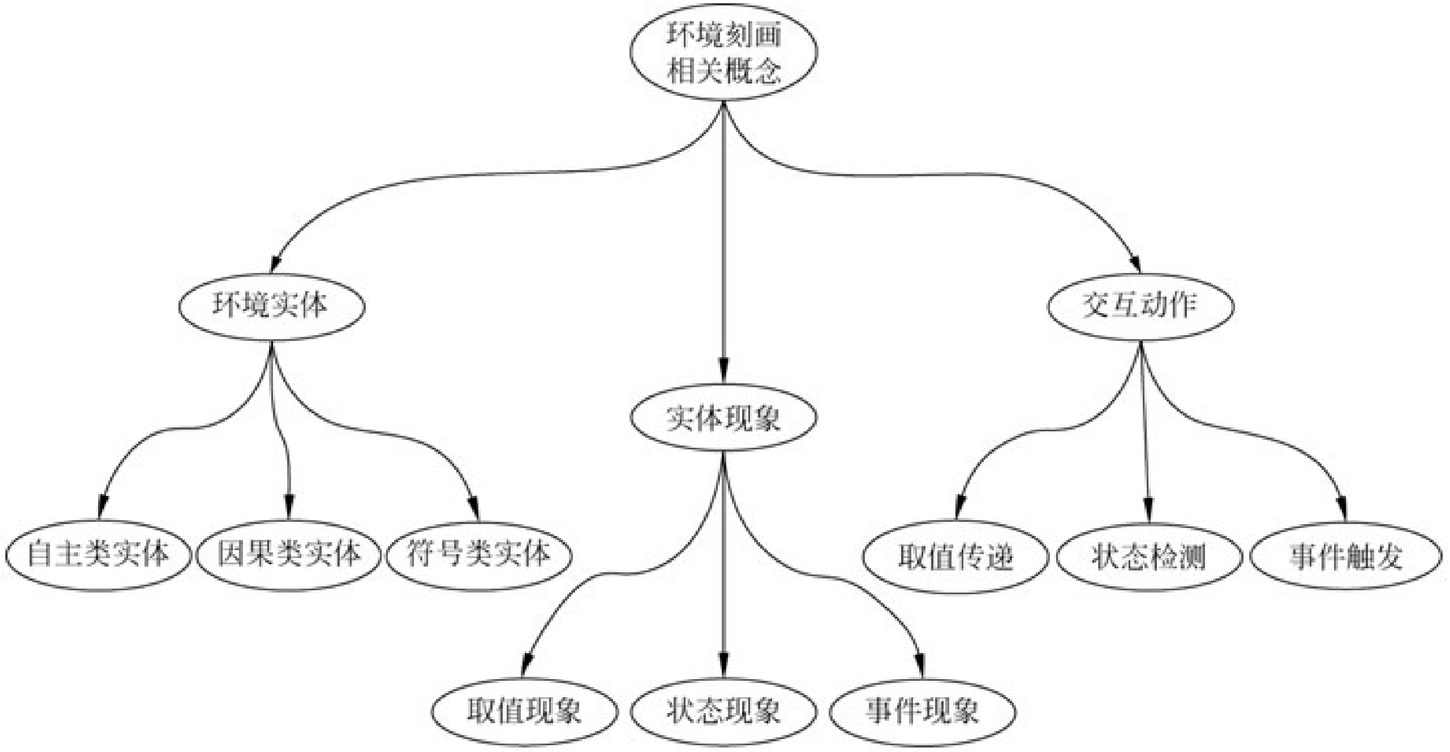


图7.2 顶层环境本体的概念分类层次

顶层环境本体

1. 环境本体的概念和关联

顶层概念关联及其含义

关　　联	关联的含义
自主类实体⇒事件现象	自主类实体有一组它可以触发的事件现象
自主类实体⇒事件触发	自主类实体可以进行事件触发动作
因果类实体⇒状态现象	因果类实体有一组可以处于的状态现象
因果类实体⇒事件现象	因果类实体有一组它可以触发的事件现象
因果类实体⇒事件触发	因果类实体可以进行事件触发动作
因果类实体⇒状态检测	因果类实体可以进行状态检测动作
符号类实体⇒取值现象	符号类实体拥有一组已经被赋值的属性
符号类实体⇒取值传递	符号类实体可以进行取值传递动作
取值现象⇒取值传递	取值现象是取值传递动作的内容
状态现象⇒状态检测	状态现象是状态检测动作的内容
事件现象⇒事件触发	事件现象是事件触发动作的内容

顶层环境本体

1. 环境本体的概念和关联

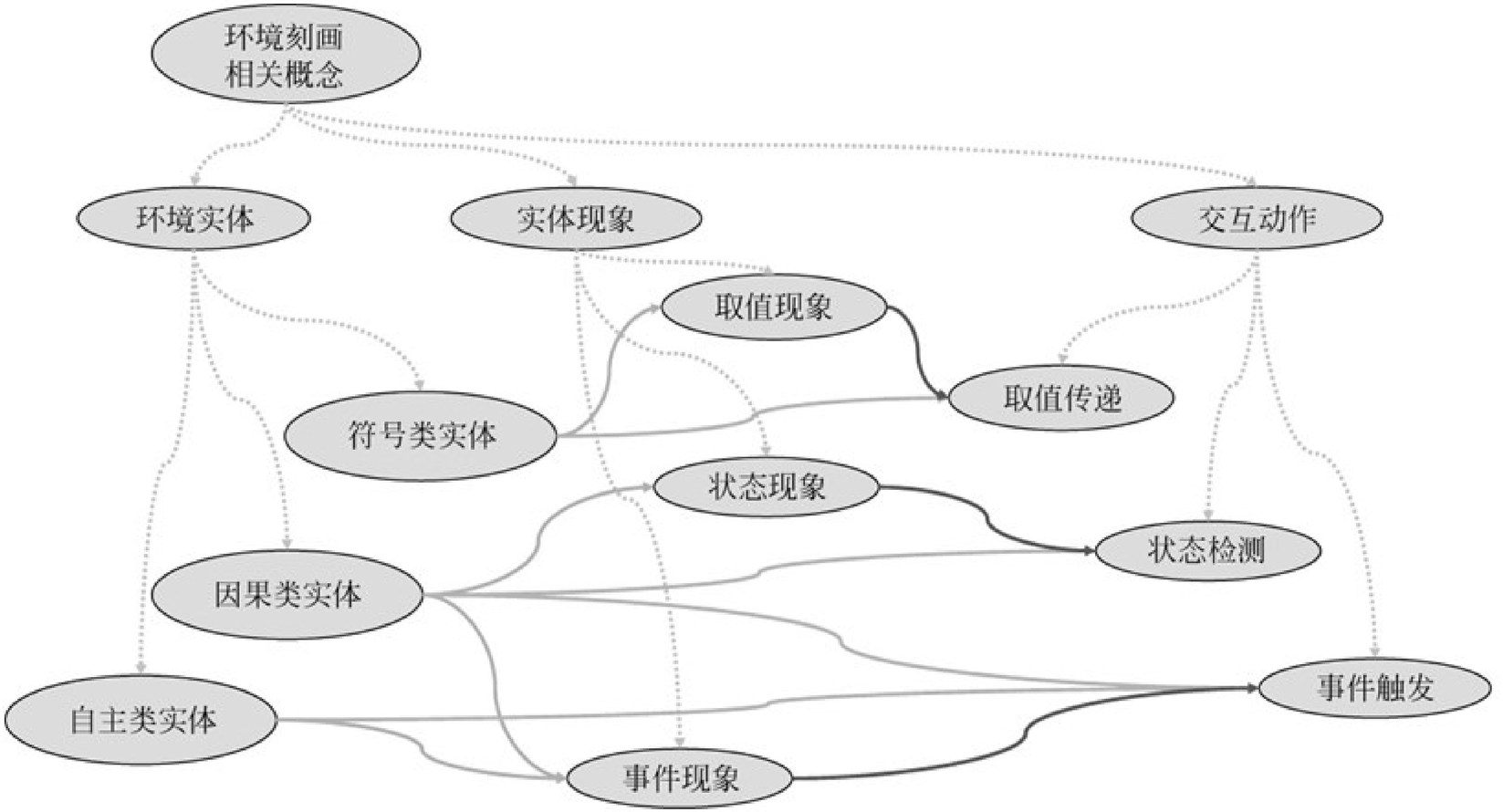


图7.3 顶层概念关联

顶层环境本体

2. 环境本体的约束集

顶层环境本体除了顶层概念及其关联外，还可以包含一组约束，即一组对概念和关联的约束，用于**表达概念和关联需要满足的条件**，在开发领域本体或者本体实例时需要遵循这些约束条件。

环境本体约束实例

1. $\forall ent_1, ent_2 \in EntSet: isa(ent_1, ent_2) \rightarrow \neg isa(ent_2, ent_1)$
2. $\forall ent_1, ent_2 \in EntSet: partof(ent_1, ent_2) \rightarrow \neg partof(ent_2, ent_1)$
3. $\forall ent \in EntSet: symbolic(ent) \rightarrow valuephe(ent, AttributeValue)$
4. $\forall ent \in EntSet: autonomous(ent) \rightarrow eventphe(ent, Event)$
5. $\forall ent \in EntSet: causal(ent) \rightarrow behavior(ent, StatesMachine)$
6. $\forall ent \in EntSet: causal(ent) \rightarrow eventphe(ent, Event)$
7. $\forall ent \in EntSet: carsal(ent) \rightarrow statephe(ent, State)$
8. $\forall sm \in StateMS: stateset(sm, ss) \rightarrow ss \neq \varnothing$
9. $\forall sm \in StateMS: transitionset(sm, ts) \rightarrow ts \neq \varnothing$
10. $\forall ent \in EntSet.\ causal(ent), behavior(ent, sm): true \rightarrow \exists s_0 \in ss.\ start(s_0), \forall s \neq s_0 \in ss.\ reachable(s_0, s)$
11. $\forall ent \in EntSet.\ causal(ent), behavior(ent, sm): stateset(sm, \{\cdots, s, \cdots\}) \rightarrow statephe(ent, \{\cdots, s, \cdots\})$
12. $\forall ent \in EntSet.\ causal(ent), behavior(ent, sm): transitionset\left(sm, \left\{\cdots, \left(s, \frac{\alpha}{\beta}, s'\right), \cdots\right\}\right) \rightarrow eventphe(ent, \{\cdots, \beta, \cdots\})$

领域环境本体

领域环境本体**结合领域概念**并通过**实例化顶层环境**本体来构建，
以智能家居系统为例,说明领域环境本体的构建过程。

1．环境实体及其类型

- 符号类实体： 如室内亮度、室内温度、室内湿度等，它们虽然是抽象的关于室内空气各项指标的度量，但在存在相应感知器的条件下，可以具有可读取的值，值的读取由相应的感知器来完成。

- 自主类实体： 如住户(人)、室内环境等，它们都是自主存在的实体。**软件系统只能接受它们触发的事件，不能对它们施加控制。**

- 因果类实体： 如窗帘、空调、各类感知器(如温度感知器、湿度感知器和光亮感知器)等。其中，对窗帘、空调和各类感知器，**软件系统可以根据其设备控制要求施加控制，它们具有可预测的行为。**

领域环境本体

2．环境实体的属性

- **符号类实体可以有取值**： 如智能家居有“室内光照度”值，合理范围一般在0.001~20000勒克斯；“室内温度”值，合理范围一般在-30摄氏度到+50摄氏度之间； “室内湿度”值，合理范围一般在10%到100%之间。

- **自主类实体可以触发事件**： 如住户(人)可以发起启动空调、关闭空调、打开窗帘、关上窗帘等事件；

- **因果类实体可以具有状态**： 如窗帘可以有“开着”和“关着”两种状态。当其处于“开着”状态时，如收到“开脉冲”事件，则保持“开着”状态，如收到“关脉冲”事件，则进入“关着”状态； 当其处于“关着”状态时，如收到“开脉冲”事件，则进入“开着”状态，如收到“关脉冲”事件则保持“关着”状态。

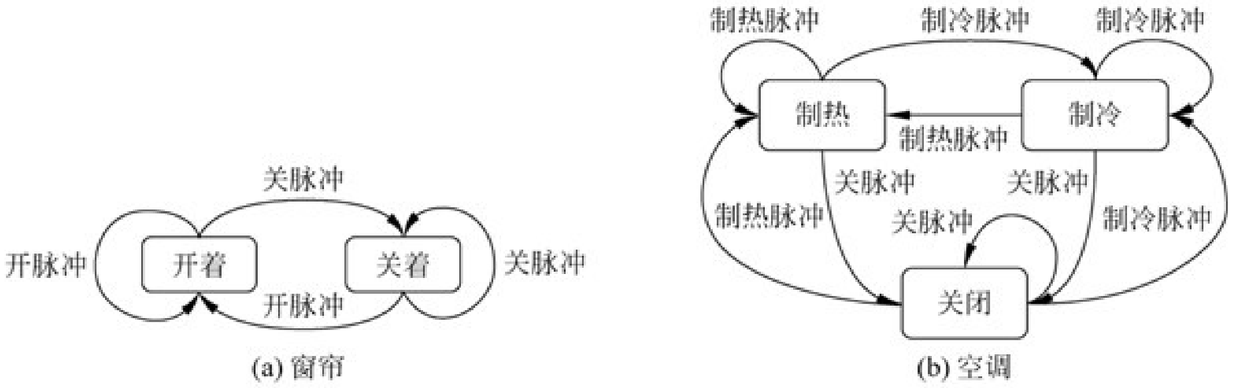


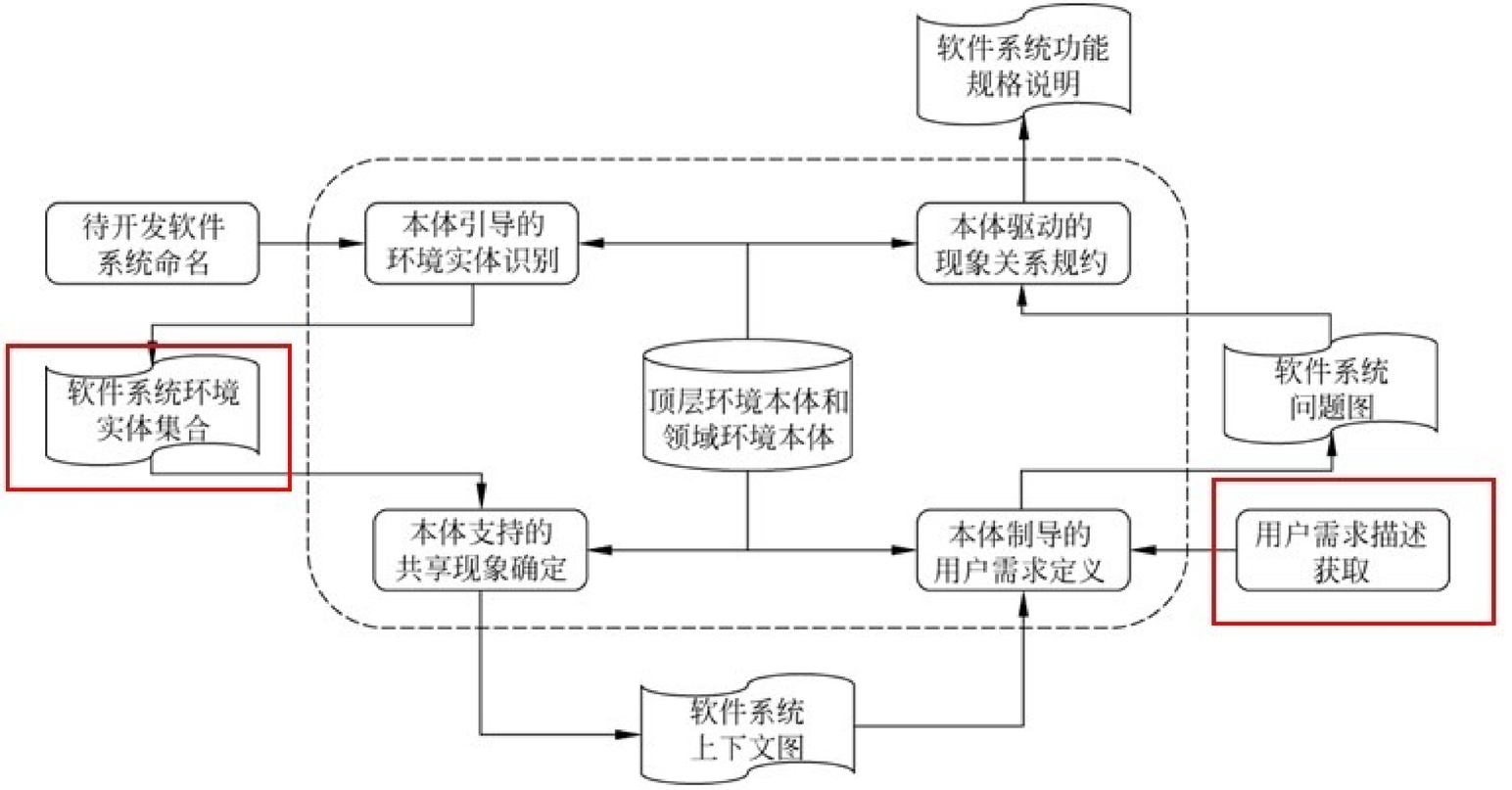
图7.4智能家居领域中部分因果实体的因果行为

软件系统问题规约

基于环境模型的软件系统问题规约，是指以问题驱动的方法为基础，以顶层环境本体和领域环境本体为支撑，根据需求描述，推断软件系统的功能规格说明。

领域环境本体制导下的问题规约过程：

- 本体引导的环境实体识别
- 本体支持的共享现象确定
- 本体制导的用户需求定义
- 本体驱动的现象关系规约



基于环境本体的需求获取过程

软件系统问题规约

案例 智能家居系统

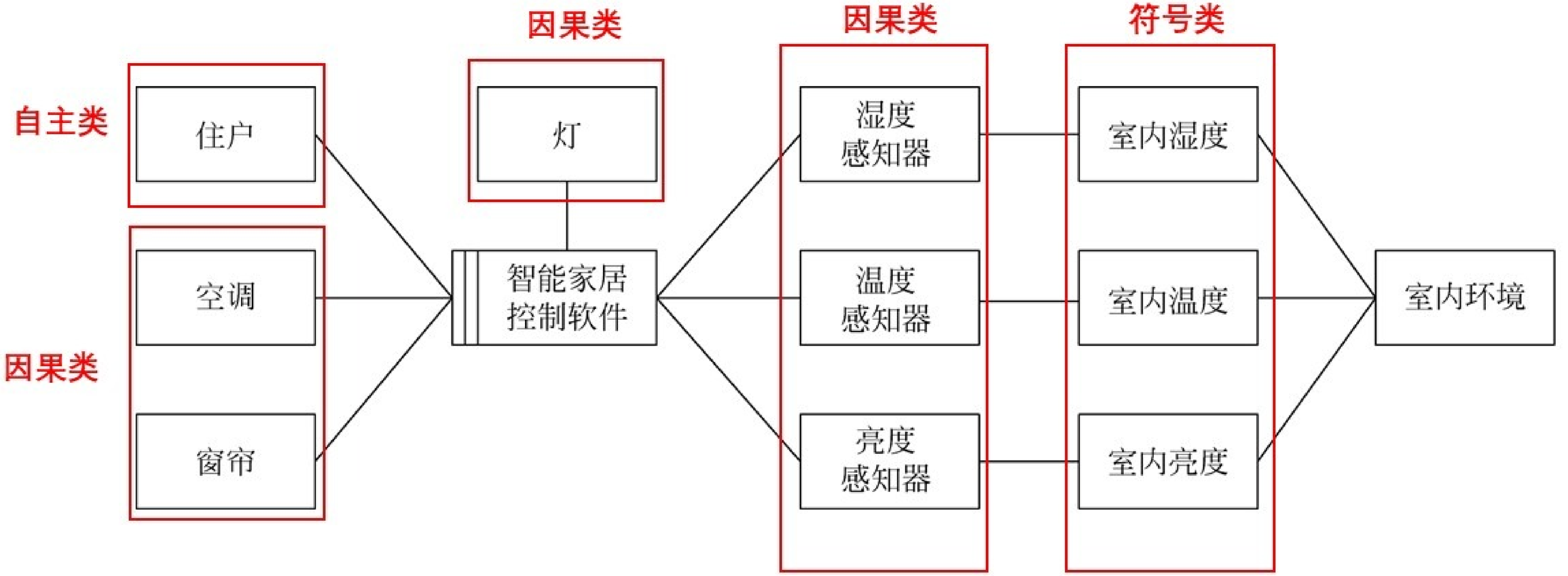
进一步细化智能家居系统的住户需求如下： (1)根据住户的命令开关空调； (2)当亮度大于30流明时关闭顶灯和台灯； (3)当温度高于25摄氏度且湿度小于25%时打开空调。

首先创建一个项目——智能家居系统，并载入智能家居的领域环境本体，然后可以开始进行智能家居系统的需求获取和规约。

本体引导的环境实体识别

- 环境实体是待开发软件系统之外的、将与该软件系统共享现象的现实世界实体。
- 可以根据其建模关注点设计相应的需求获取问卷，用于指导对待开发软件系统的环境实体的识别和建模。
  - **针对可能的符号类实体,需要考察**：待开发软件系统是否需要从它们那里获取信息或数据？它们是否使用待开发软件系统产生的信息或数据？如果需要,则将这样的符号类实体确定为待开发系统的外部环境实体,将需要传递的信息或数据识别为交互现象;
  - **针对可能的自主类实体,需要考察**：它们是否使用待开发软件系统？待开发系统是否需要它们来维护或管理？待开发软件系统是否需要了解或掌握该类实体的状况?如果待开发软件系统与这些自主类实体之间存在交互,则这些实体很可能需要成为待开发软件系统的外部环境实体,其间发生的使用、管理和感知等事件将被识别为交互现象;

本体引导的环境实体识别



智能家居控制软件的简化上下文图

本体支持的共享现象确定

（1） 识别待开发软件系统与外部环境实体之间的共享现象

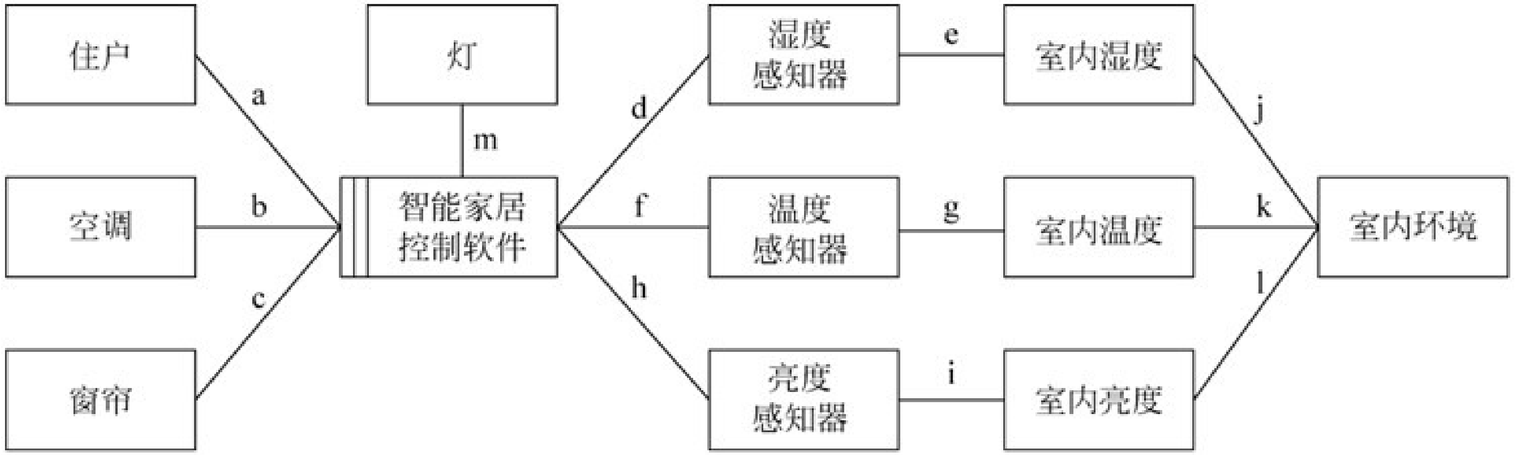
例 基于智能家居各环境实体类型和智能家居环境本体，可以诱导出如下需求相关信息。

① “住户［A］”发出让空调制冷、制热或关闭空调等命令；
② “室内环境［A］”与“室内温度［S］”“室内湿度［S］”“室内亮度［S］”分别具有可共享的“温度值”“湿度值”和“亮度值”；
③ “室内温度［S］”“室内湿度［S］”“室内亮度［S］”分别通过“温度感知器”、“湿度感知器”和“亮度感知器”共享室内温度、室内湿度和室内亮度样本，而这些感知器与待开发智能家居控制软件共享“温度信号”“湿度信号”与“亮度信号”；
④ “空调［C］”和待开发智能家居控制软件共享的现象有“制冷脉冲”“制热脉冲”和“关闭脉冲”等事件，通过它们才能够打开空调制冷模式、制热模式和关闭空调；
⑤ “窗帘［C］”和待开发智能家居控制软件共享的现象有“窗帘关脉冲”和“窗帘开脉冲”事件，通过它们才能打开或关闭窗帘，这从领域环境本体中获取；
⑥ “灯［C］”和待开发智能家居控制软件共享的现象有“关灯脉冲”和“开灯脉冲”事件，通过它们才能够开灯或者关灯。

本体支持的共享现象确定

（2） 识别接口

例 住户发起命令，与待开发智能家居控制软件共享，现象类型都是事件，现象都由住户发起，由待开发智能家居控制软件接收。由此可以定义接口a。类似地，可以识别其他接口。经过步骤“本体引导的环境实体识别”和“本体支持的共享现象确定” 之后，得到待开发智能家居控制软件的上下文图。



a: 住户!{制热命令，制冷命令，关闭命令} b: 智能家居控制软件!{制热脉冲，制冷脉冲，关闭脉冲}，空调!{制热，制冷，关闭} c: 窗帘!{打开，关闭}智能家居控制软件!{开脉冲，关脉冲} d: 湿度感知器!{湿度信号}
e: 室内湿度!{空气湿度样本}f: 温度感知器!{温度信号} g: 室内温度!{空气温度样本} h: 亮度感知器!{亮度信号}
i: 室内亮度!{亮度样本}j: 室内环境!{湿度值} k: 室内环境!{温度值} l: 室内环境!{亮度值}
m: 智能家居控制软件!{关灯脉冲}

本体制导的用户需求定义

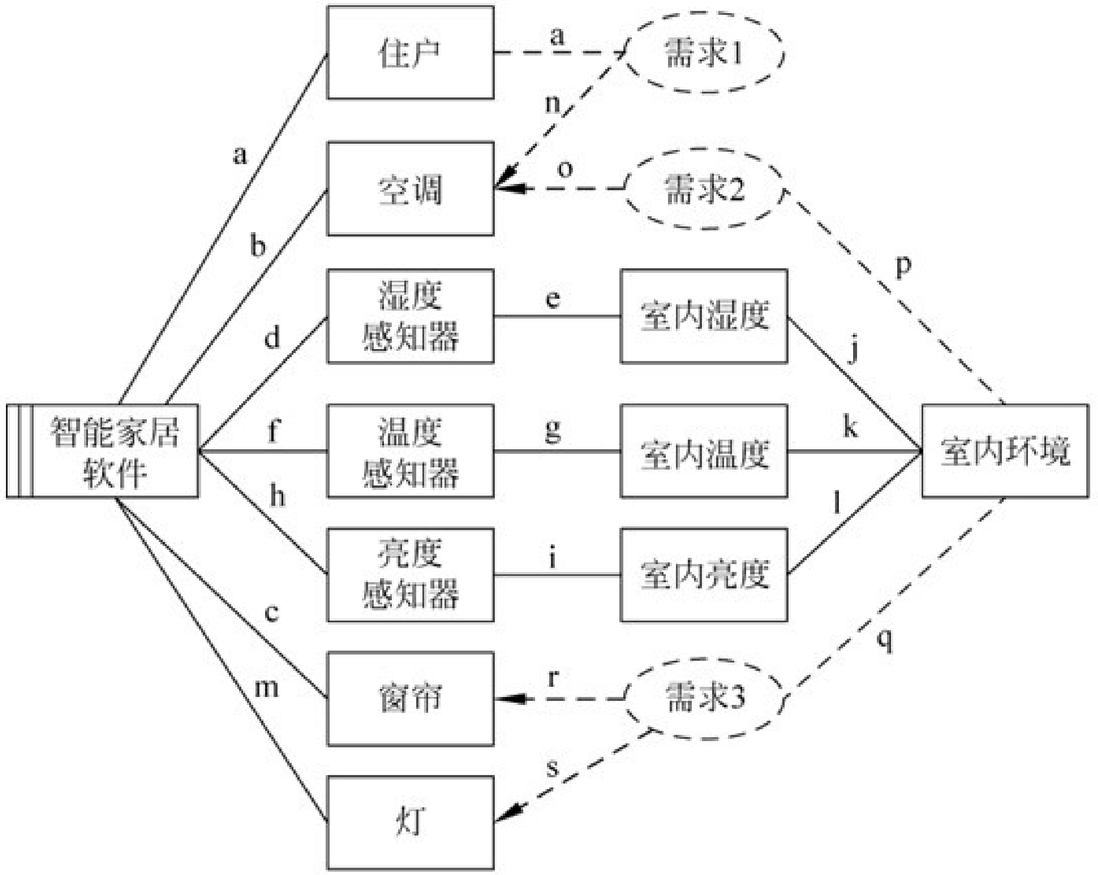
（1）获取用户需求描述

例 智能家居控制软件问题中期望要满足的三个约束关系是： ①如果住户主动对空调实施操作，则根据住户的命令开关空调； ②当室内温度高于25摄氏度且室内湿度小于25%时空调应设置为制冷模式； ③当室内亮度大于30流明时窗帘和灯都应处于关闭状态。

（2） 识别需求引用和需求约束

例 为满足需求1“根据住户的命令开关空调”，要看每个环境实体在该需求下的用户期望现象。这个需求跟“住户”和“空调”两个环境实体相关。从智能家居领域环境本体中可以得知，自主类实体“住户”会发出“制热”、“制冷”和“关闭”等命令事件，智能家居系统需要接收这些命令，并进行相应的动作，这些是用户期望的需求引用。

本体制导的用户需求定义



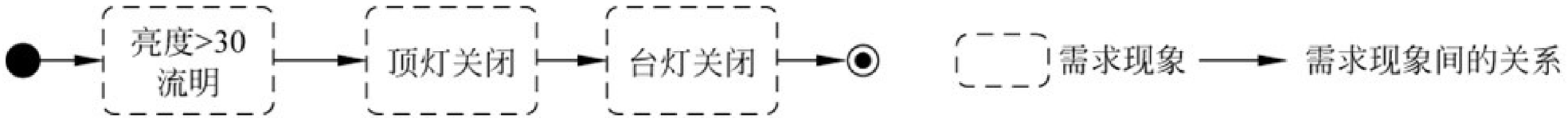
智能家居控制软件的问题图

a: 住户!{制热命令，制冷命令，关闭命令}
b: 智能家居软件!{制热脉冲，制冷脉冲，关闭脉冲}，空调!{制热，制冷，关闭}
c: 窗帘!{窗帘打开，窗帘关闭}智能家居软件!{开窗脉冲，关窗脉冲}
d: 湿度感知器!{湿度信号}
e: 室内湿度!{空气湿度样本}
f: 温度感知器!{温度信号}
g: 室内温度!{空气温度样本}
h: 亮度感知器!{亮度信号}
i: 室内光亮!{亮度信号}
j: 室内环境!(湿度值)
k: 室内环境!{温度值}
l: 室内环境!{亮度值}
m: 灯!{灯打开，灯关闭}，智能家居软件!{开灯脉冲，关灯脉冲}
n: 空调!{制热，制冷，关闭}
o: 空调!{制冷，关闭}
p: 室内环境!{温度>25摄氏度，温度>25%}
q: 室内环境!{亮度>30流明}
r: 窗帘!{窗帘关闭}
s: 灯!{灯关闭}
需求1: 按住户命令控制空调
需求2: 温度高于25摄氏度且湿度小于25%则开冷空调
需求3: 亮度大于30流明则关闭窗帘和灯

本体驱动的现象关系规约

(1) 定义需求发生序列

例 以需求 (当室内亮度大于30流明时顶灯和台灯都应处于关闭状态)为例，当亮度大于30流明时，用户期望看到顶灯和台灯都是关着的。



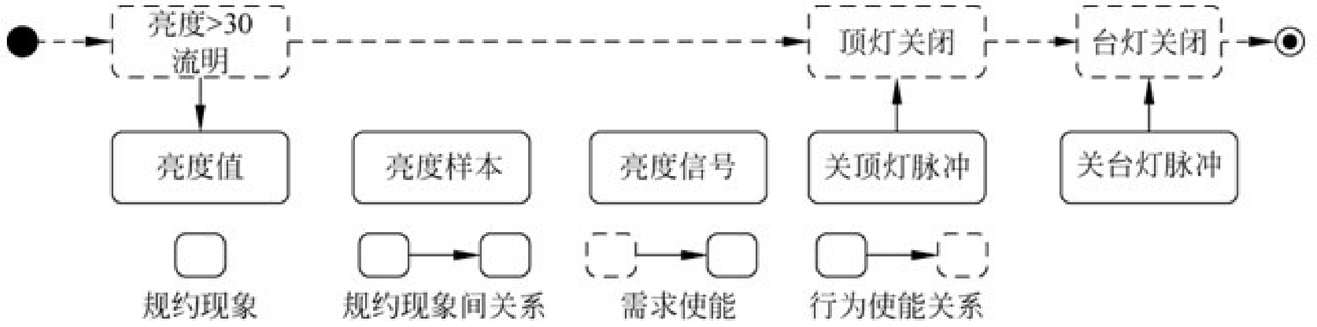
图定义需求3发生序列的需求活动图

本体驱动的现象关系规约

（2）获取需求现象与规约现象间关系

需求现象与规约现象间有如下三种关系。

- 行为使能关系：指系统行为规约现象使能需求现象的发生，例如制冷脉冲会让空调的状态变为制冷状态。
- 需求使能关系：指需求现象使能系统行为规约现象的发生，例如想要知道当前室内温度值，需要获取温度传感器传来的信号。
- 同步关系：指系统行为规约现象与需求现象可以同时发生。



智能家居控制软件的需求3中需求现象与规约现象间的关系

本体驱动的现象关系规约

获取规约现象间关系

例 手动排序其他的系统行为规约现象，可以抽取出需求3的系统行为规约。

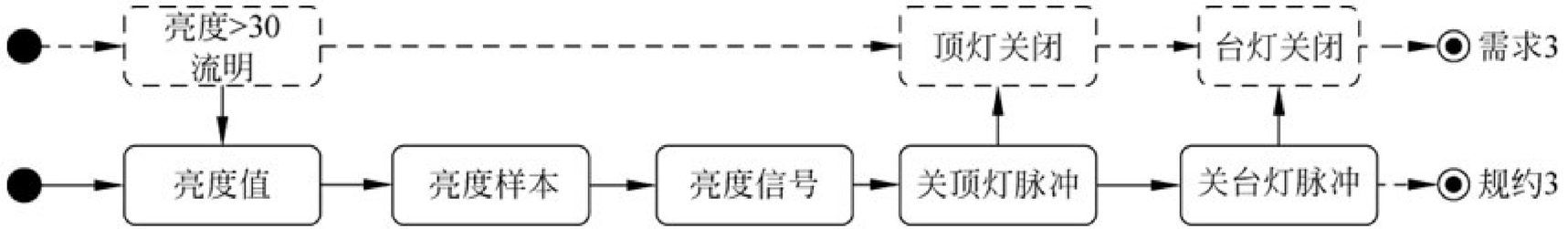


图7.11智能家居控制软件从需求3中抽取规约3的示意图

环境相关的典型非功能需求

环境模型需要反映现实世界的复杂性，定义各种各样的性质和约束，这些不同类型的环境特性和约束都可能预示不同的非功能需求关注点。

典型的由环境特性引出的非功能需求：

(1) 环境不确定性与自适应性。

(2) 环境时间特性与时间约束。

(3) 环境脆弱性与公共安全需求。

(4) 环境威胁与信息安全需求。

(5) 环境信息敏感性与隐私保护需求。

环境相关的典型非功能需求

环境不确定性与自适应性

环境相关的典型非功能需求

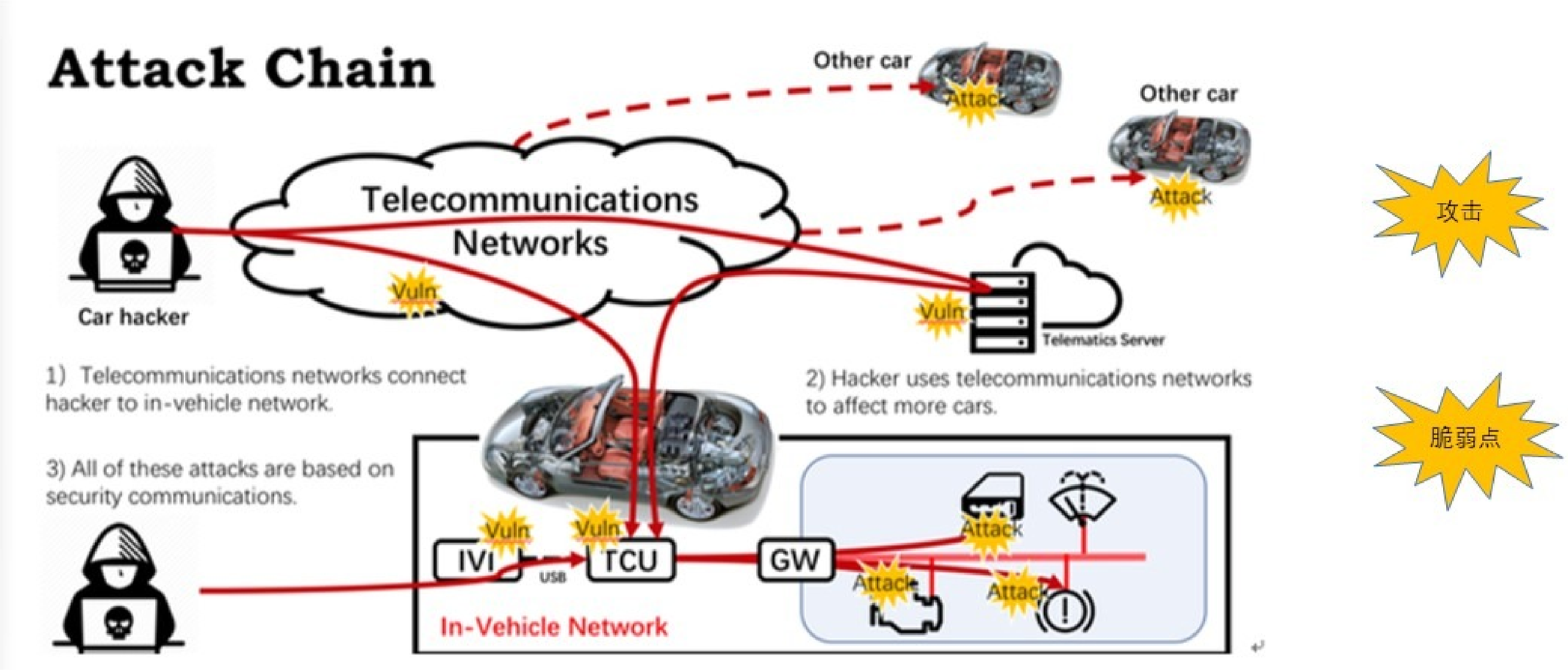
环境时间特性与时间约束

环境相关的典型非功能需求

环境脆弱性与公共安全需求

环境相关的典型非功能需求

环境威胁与信息安全需求

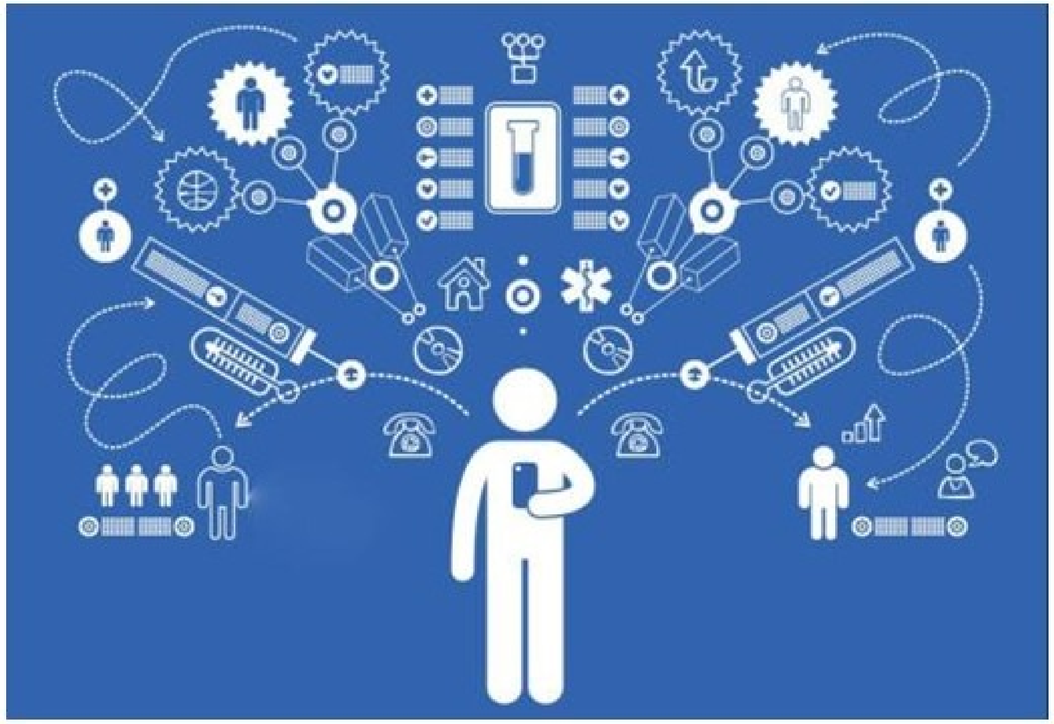


攻击

脆弱点

环境相关的典型非功能需求

环境信息敏感性与隐私保护需求



小结与讨论

- 介绍了基于环境建模的需求工程方法的基本思想

仅仅给出了离散的环境模型，在实际项目中可以针对特定的建模关注点，对环境模型进行扩展。例如，可以使用时间自动机对时间特性进行扩展，使用随机混成自动机对不确定进行扩展，等等。

- 介绍了基于环境模型的功能需求获取

而实际上基于环境模型可以做更多的事情，如系统能力的刻画、系统能力的比较和组合、系统能力的精化、系统能力的聚合等。

- 介绍了环境特性带来的典型非功能需求

如何在环境模型的支持下，具体研究每种非功能需求及多种非功能需求约束下的行为，都是有意义的研究课题。

思考题

1. 请遵循领域环境本体制导下的问题规约过程，对智能会议室系统进行问题规约。

智慧会议室系统会自动读取预订系统中的会议信息。在有预订会议的时间段内，如果有人进入会议室，则会自动打开窗帘；若有人接近屏幕，则自动打开屏幕，关闭窗帘，打开灯，启动开会模式。会议结束后，人离开会议室，则所有设备全部自动关闭。

2. 请根据如下描述，构建智能马桶的领域环境本体，并根据该本体进行问题规约。

智能马桶包括四个部分：冲水单元(Flusher Unit)、清洗单元(Washing Unit)、加热单元(Heating Unit)和智能马桶盖(Toilet Cover)。这些部分分别由冲洗控制器(Flusher Operator)、清洗控制器(Washing Operator)、加热控制器(Heating Operator)和红外传感器(Infraed Sensor)控制。对于冲水单元、清洗单元和加热单元，其控制器按钮可以控制该单元的开关；而智能马桶盖会通过红外传感器感知人的位置，当使用者靠近时会自动打开，而使用者远离时会自动合上。