质量需求分析

徐思涵

南开大学

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

浏览器案例

- 核心功能需求
  - 根据用户的请求，获取并展示信息
- 质量需求
  - 载入速度
  - 数据跨平台同步
  - 用户隐私
  - ……

满足功能需求是软件项目成功的必要条件（保证了下限）

质量需求的满足程度决定了软件的上限

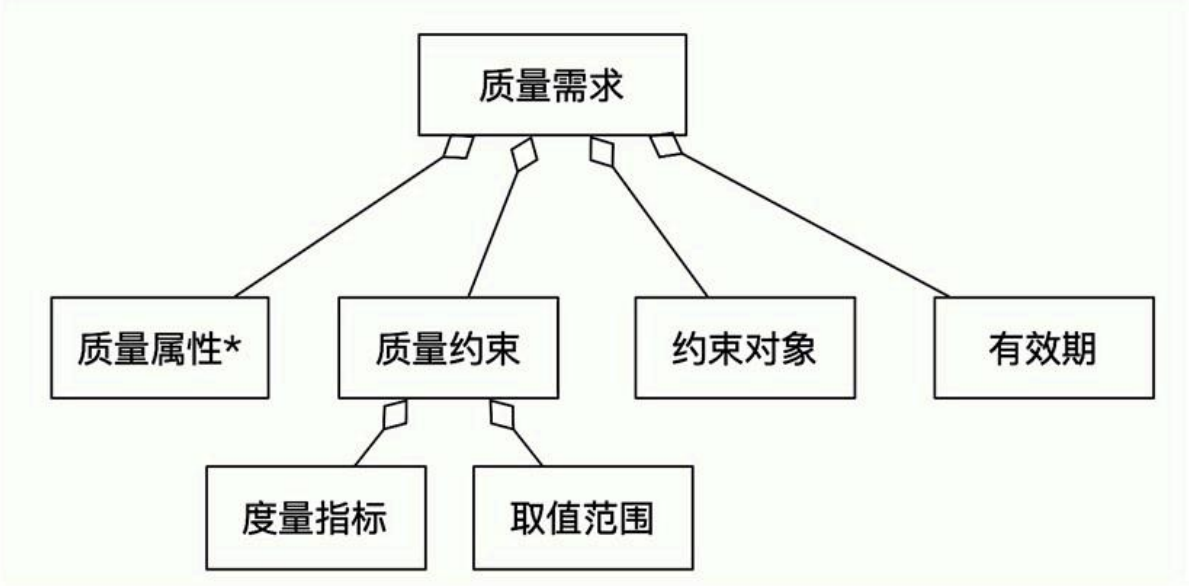
不同的浏览器有什么异同？如何在竞品中脱颖而出？

质量需求分析的难点

- 主观性
  - 不同的人对它有不同的看法、不同的解释、甚至不同的评判方式
- 多样性
  - 同一质量需求在不同类型系统中的重要性大相径庭
- 耦合性
  - 质量需求之间常常相互影响，满足了一个质量需求可能会影响其它质量需求的可满足性，如，安全性和易用性

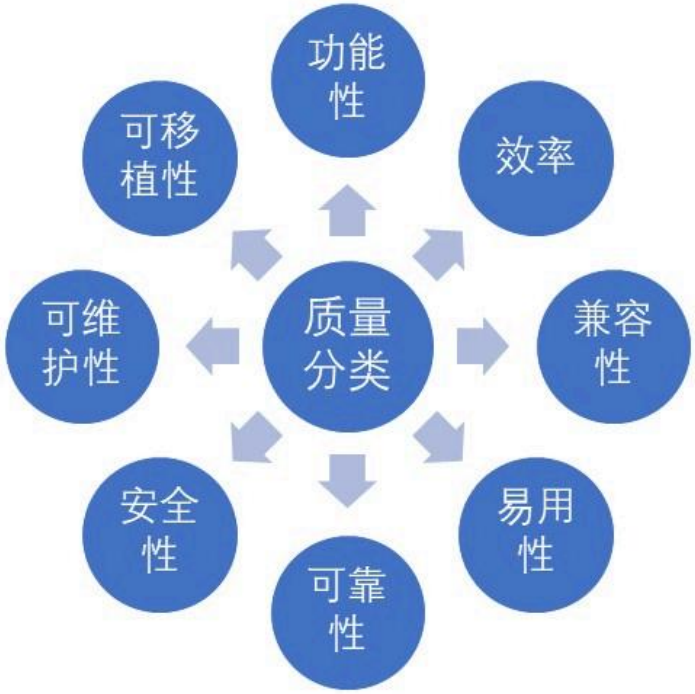
质量需求定义

- 质量需求是对系统（功能）的质量期望的描述，包括：
  - 质量属性
  - 质量约束
  - 约束对象
  - 有效期



质量需求定义

- 质量需求
  - 对系统特定质量属性的要求，如性能、安全性、可扩展性、可用性等
- 质量属性分类
  - 国际标准 ISO/IEC 25010:2011中涵盖，8 大类质量属性



质量需求定义

- 质量约束
  - 基于度量指标和取值范围，针对特定质量属性进行约束，以表示希望在该质量属性维度应达到的程度

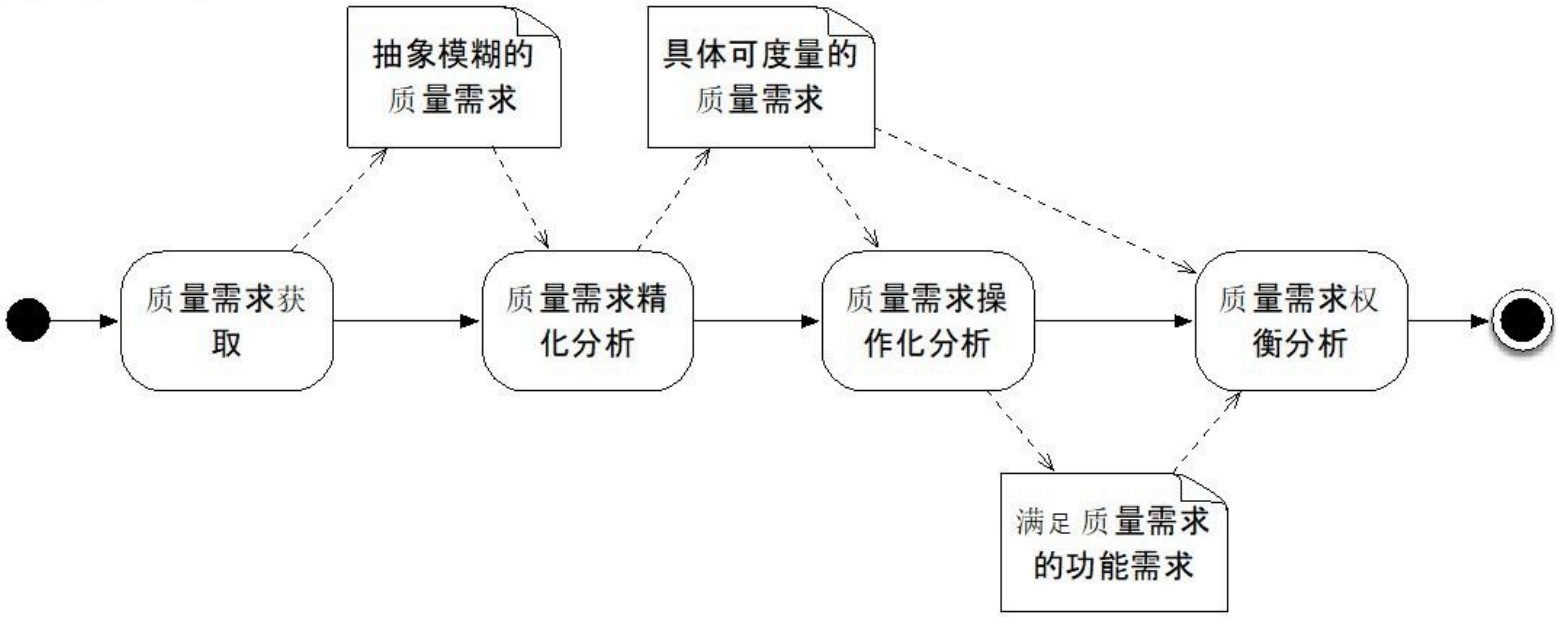
质量属性	常用度量指标
效率	每秒钟处理的事务数；用户输入的响应时间
可靠性	功能点失效出现的频率；失效的平均时间;平均无故障时间
易用性	用户操作所需的时间；操作出现错误的频度；操作次数
可维护性	诊断和改正系统错误的成本
兼容性	系统能够兼容的系统平台数量；系统能够兼容的版本的数量
安全性	系统信息泄露的次数；系统成功防御外部攻击的次数
可移植性	原程序设计和调试的成本与移植所需费用的比值
功能适配性	能够满足用户需求的功能点数量

质量需求定义

- 约束对象
  - 质量约束需施加于特定客体（即约束对象），表达对其的约束
  - **约束对象可以是整个软件系统，也可以是某个系统模块或特定功能，或是与系统运行相关的物理或信息资产**
- 有效期
  - 系统干系人对同一质量的需求在不同时期可能不相同，准确地分析和提炼质量需求的约束时间区段能 够有效地降低系统开发成本
  - 如，高考考题在考试前对其保密性的要求非常高。而在考试结束后考题可以公开

质量需求分析过程

- 质量需求分析：将抽象的质量需求，转换为**可度量**的系统特性描述的过程



质量需求分析过程

- **质量需求获取**：用户通常只能比较含糊地表达他们所关注的问题，通过分析**用户关注点**能够有效获取初始的系统质量需求
- **质量需求精化**：**质量需求所约束和影响的范围越广，满足该需求的代价就越高。**通过对质量需求进行精化分析，能够准确地识别出系统干系人的细粒度质量需求，从而更加精准地设计系统功能以满足质量需求
- **质量需求操作化**：将质量需求精化到可度量的细粒度需求后，需要通过操作化分析来**设计能满足该质量需求的设计方案**
- **质量需求权衡**：当质量需求的操作化存在多种方案时，需要对不同质量进行权衡，形成**最优决策方案**

智能电网实时定价场景

基于智能电网进行实时定价能够动态改变用电需求，从而有效引导用户用电行为，减少高峰用电，防止意外停电。具体地:电力供应商收集实时能耗数据，根据相应的电价情况适时调整用电模式，从而平衡电网负载，优化电力基础设施的运行和管理。其中，**用电信息收集和定价决策是关键。**

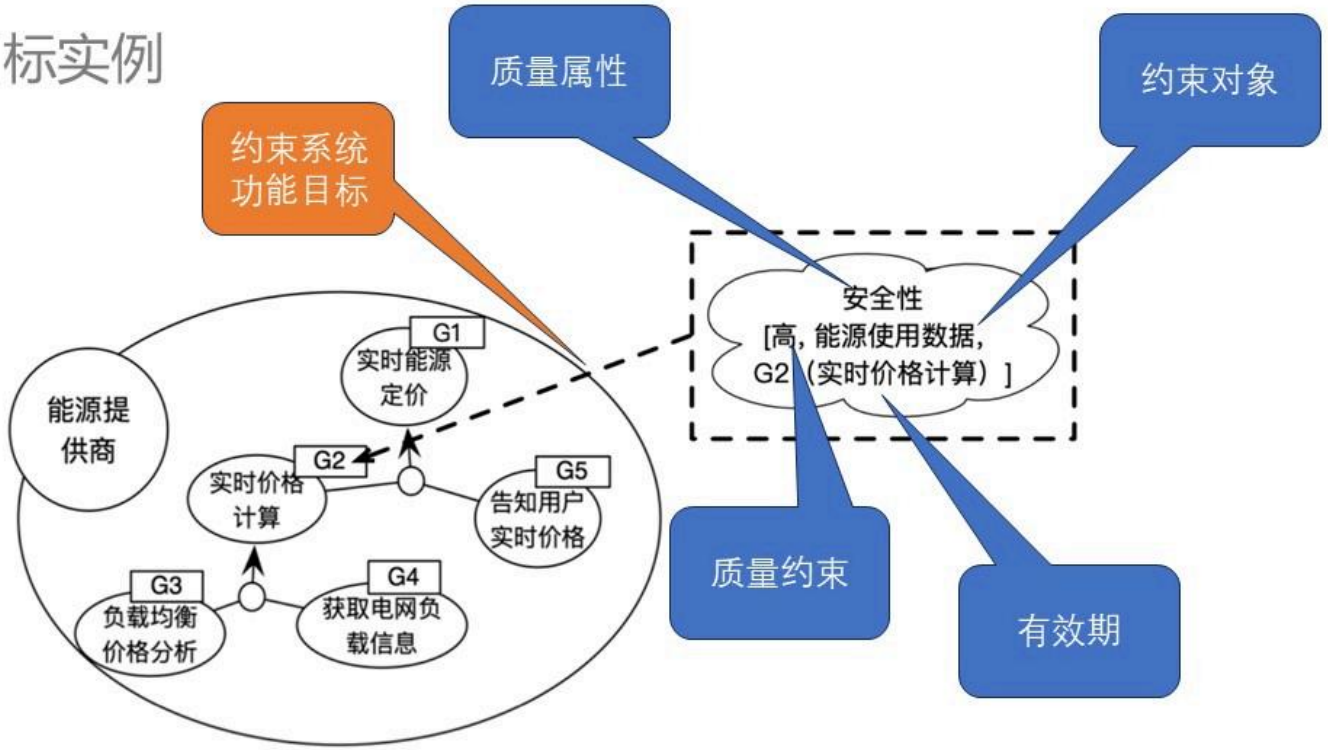
质量目标定义与建模

- 质量目标定义
  - 质量目标表示系统干系人期望系统达到的某种程度的质量
  - 基于扩展巴科斯范式的（EBNF）质量目标定义

<质量目标> ::= <质量属性>, <质量描述>*	（定义 1）
<质量描述> ::= <描述维度>, <描述信息>	（定义 2）
<描述维度> ::= ‘质量约束’ | ‘约束对象’ | ‘有效期’	（定义 3）

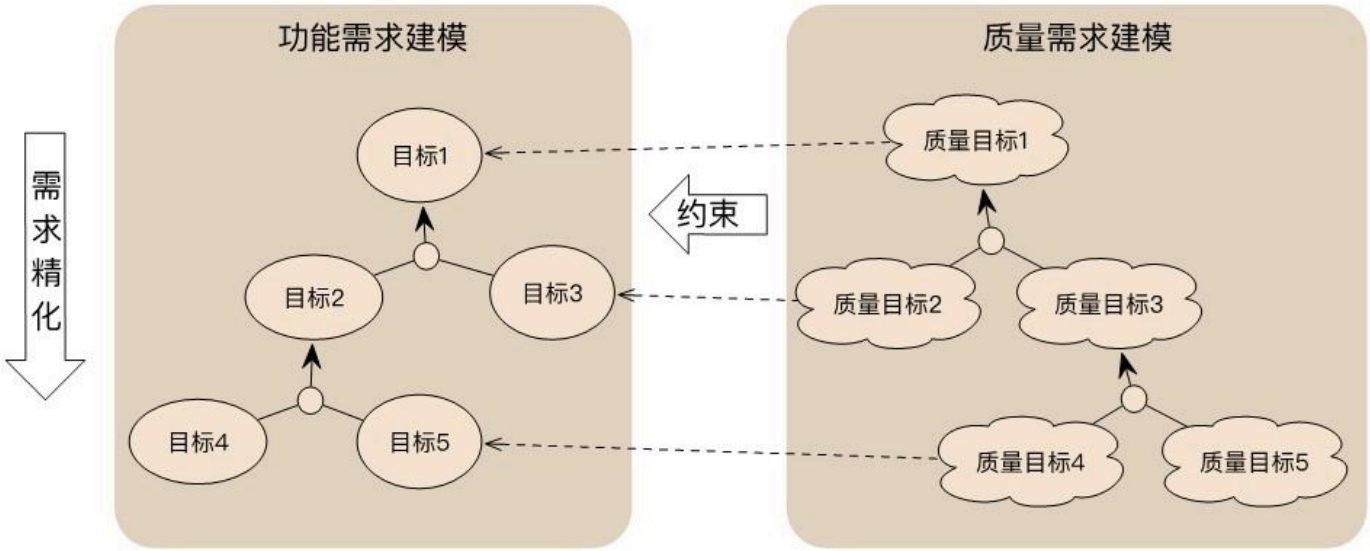
质量目标定义与建模

- 质量目标实例



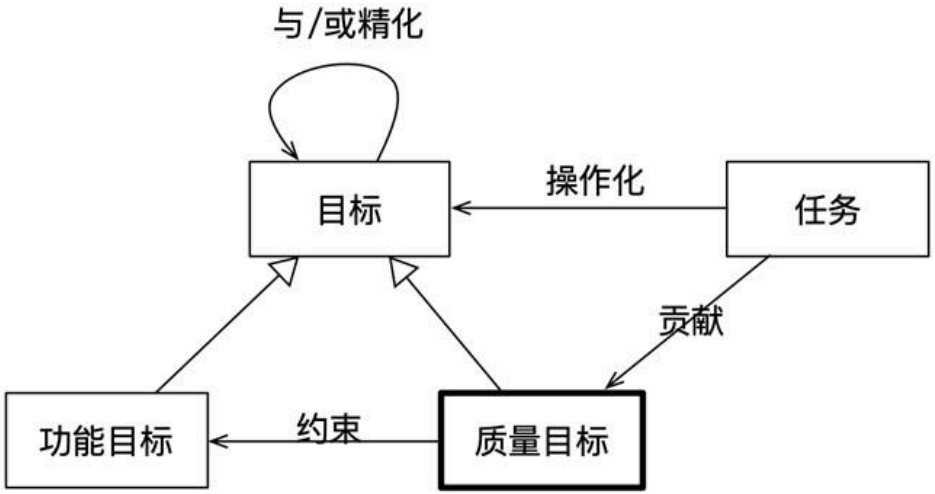
质量目标与功能目标的关联建模

- 质量需求是对系统或其特定功能的约束，**质量需求不能独立存在**，而应关联到所约束的系统功能需求上



质量目标关系建模

- 质量需求建模将质量目标作为建模的核心元素
  - 复用面向目标方法中的精化关系、操作化关系、以及贡献关系



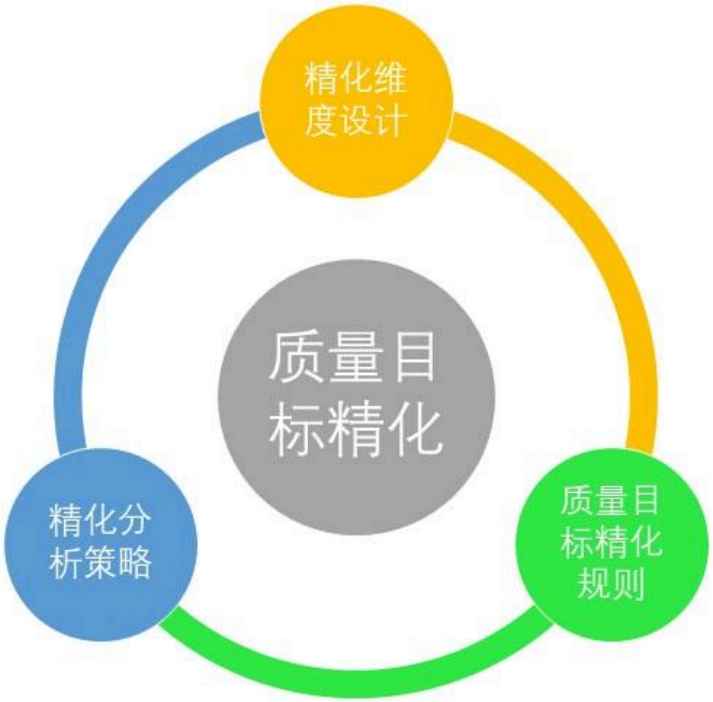
质量目标的精化关系

- 精化关系
  - 精化关系将抽象的质量目标通过“与/或精化”得到更细粒度的质量目标，从而能关注到更具体的质量描述，并施加更具体的质量约束。
  - 与功能目标精化关系的相似之处：
    - 若子目标之间是“与”关系，所有子目标被满足，父目标才满足
    - 若子目标之间是“或”关系，只要一个子目标被满足，父目标即可被满足
  - 与功能目标精化关系的不同之处：
    - **质量目标所关注的质量属性通常不依赖于具体领域，即每种质量属性有相对固定的子属性。**例如，安全性包括机密性、完整性和可用性三个子属性（CIA 模型）

质量目标的操作化关系和贡献关系

- 操作化关系
  - 质量目标是对特定功能的质量约束，操作化关系展示了质量目标如何通过具体的任务来满足。
  - 例，家庭用电数据在传输过程中应保证用户用电的个人隐私（质量目标）为此需要对家庭用电数据进行加密操作（任务）
- 贡献关系
  - 操作化的任务一方面可以满足该质量目标，另一方面还会对其他质量目标产生正向或负向的影响， 形成贡献关系。
  - 例，在家庭用电数据传输过程中执行加密操作能满足家庭用电数据的保密性，但同时会对性能产生一定的消极影响，即存在对性能的负向贡献关系

总体框架



质量目标的精化维度设计

- 不同质量需求涉及到不同的领域知识，对不同质量目标进行精化分析，需要首先基于领域特征确定质量目标的精化维度

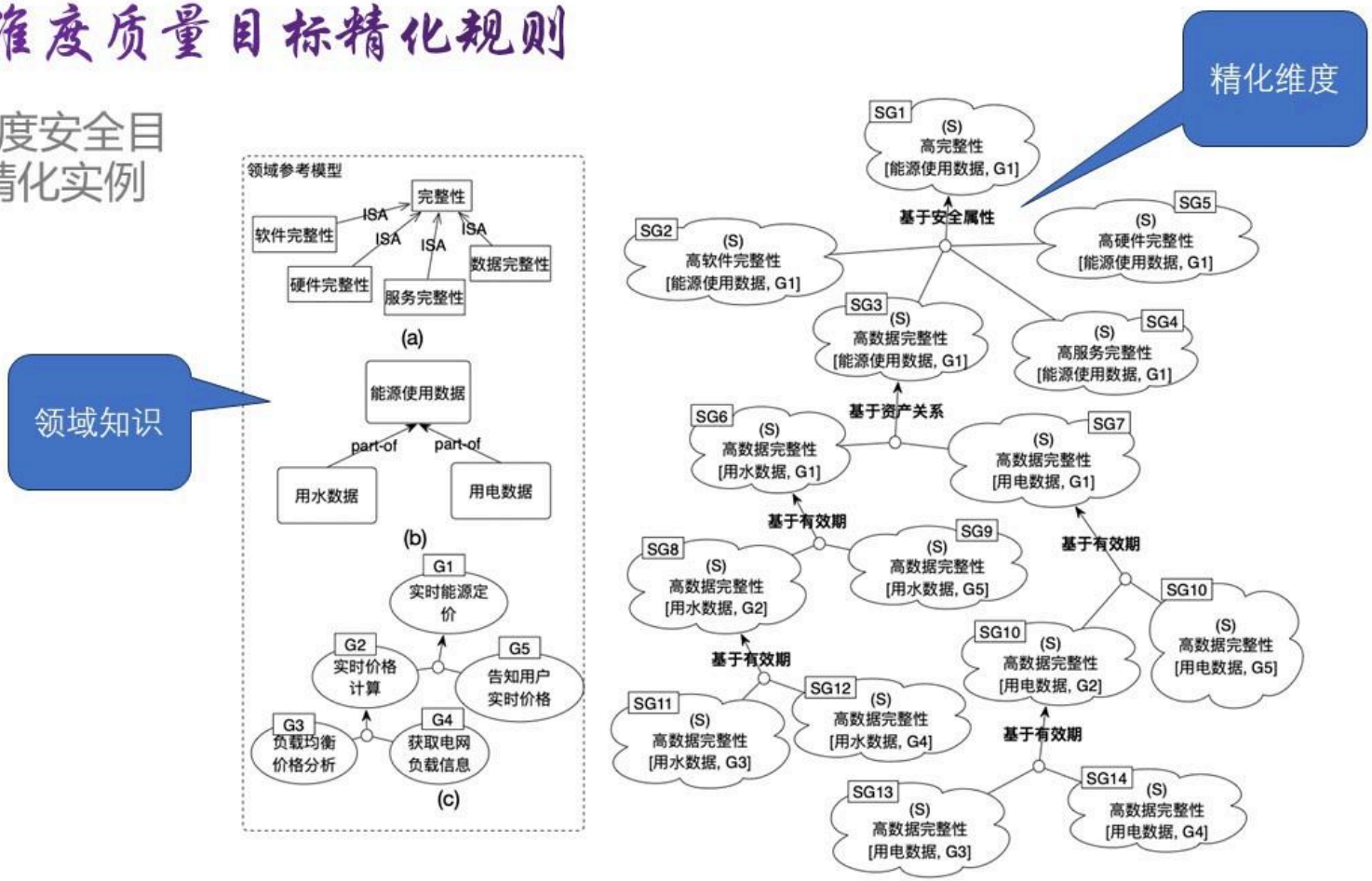
- 以安全领域为例，**安全目标的精化维度**
  - 重要性：对安全性重要程度的定性约束（高、中、低等）
  - 安全属性：机密性，完整性，和可用性（CIA 模型）
  - 资产：任何对系统干系人有价值的东西，数据、软硬件或服务等
  - 有效期：安全目标所施加安全约束的时间段，以系统特定功能目标的执行阶段来刻画

多维度质量目标精化规则

- 基于质量目标的精化维度，通过“与或精化关系”将抽象的质量目标细化为具体精确的目标
  - 基于安全属性的安全目标精化：根据安全属性之间的泛化关系，将安全约束由父属性扩展传播到子属性上
  - 基于资产关系的安全目标精化：根据资产之间的整体-部分关系，针对具体资产在不同业务场景中的使用情况，分析其细粒度的安全目标
  - 基于有效期的安全目标精化：考虑安全目标与特定功能目标相关联（即它在该特定功能目标被执行和满足的时间周期内施加约束），进行精化分析

多维度质量目标精化规则

多维度安全目标精化实例



质量目标精化分析策略

- 精化分析的粒度（合适停止精化分析？）
  - 判断标准1：是否具备精化分析的领域知识
  - 判断标准2：精化后的细粒度质量目标是否能被操作化为具体的任务措施
  - 判断标准3：精化后的细粒度质量目标是否全部为无效目标
- 精化后质量目标的有效性判断
  - 判断标准1：与系统干系人进行沟通，确认是否需要精化后目标
  - 判断标准2：基于领域分析，评估质量目标的必要性。如，安全目标分析时通常基于**风险分析**来判断安全目标所面临的风险
    - 安全风险 = 威胁发生概率 ´ 威胁严重程度

本章小结

- 功能需求定义软件系统的刚性要求，决定软件系统的下限；质量需求定义软件系统的柔性要求，决定软件系统的上限
- 质量需求是施加于功能需求之上的约束，不可独立存在
- 质量需求分析框架能够有效地将功能需求与质量需求相关联，基于目标模型自顶向下逐步求精的机制，支持系统地对结构化表示的质量需求进行精化分析，并最终获得可操作化的质量需求

思考题

1. 请分别介绍 1 款你认为好用和不好用的软件，并分析这两款软件满足或不满足哪些质量需求。
2. 某软件开发的需求文档中包含以下质量需求“系统应具有高可靠性，能够应对潜在的风险”。请分析该需求的问题，并给出解决该问题的方 法。
3. 请利用质量需求的精化分析方法，分析用户对于即时通讯软件的易用性需求，列出精化后的易用性需求。
4. 针对第 2 题中所得到的细化的易用性需求，分析这些需求可以被操作化为哪些具体的软件功能或软件样式设计。

思考题（续）

5. 请查阅软件易用性的相关知识，定义 一种易用性模式

6. 质量需求之间可能存在冲突，请给出一个包含冲突的质量需求的例子

7. 质量需求应与功能需求同时分析，还是先分析功能需求再分析质量需求?请阐述原因

参考文献

1. Chung, L., Nixon, B. A., Yu, E., and Mylopoulos, J. (2012). Non-functional requirements in software engineering (Vol. 5). Springer Science & Business Media.
2. Li, F. L., Horkoff, J., Mylopoulos, J., Guizzardi, R. S., Guizzardi, G., Borgida, A., and Liu, L. (2014). Non-functional requirements as qualities, with a spice of ontology. In 2014 IEEE 22nd International Requirements Engineering Conference (RE) (pp. 293- 302). IEEE.
3. Glinz, M. (2007). On non-functional requirements. In 15th IEEE International Requirements Engineering Conference (RE 2007) (pp. 21-26). IEEE.
4. Liaskos, S., Yu, Y., Yu, E., and Mylopoulos, J. (2006). On goal-based variability acquisition and analysis, Proceedings of 14th IEEE International Conferenceof Requirements Engineering, RE 2006: 79-88, IEEE.
5. Horkoff, J., and Yu, E. (2013). Comparison and evaluation of goal-oriented satisfaction analysis techniques. Requirements Engineering, 18(3): 199-222

参考文献（续）

6. Gross, D., & Yu, E. (2001). From non-functional requirements to design through patterns. Requirements Engineering, 6(1), 18-36.
7. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., and Sommerlad, P. (2013). Security Patterns: Integrating security and systems engineering. John Wiley & Sons.
8. Li, T., Horkoff, J., and Mylopoulos, J. (2018). Holistic security requirements analysis for socio-technical systems. Software & Systems Modeling, 17(4):1253-1285. 9. Fernandez-Buglioni, E. (2013). Security patterns in practice: designing secure architectures using software patterns. John Wiley & Sons.

需求验证

徐思涵

南开大学

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

需求的形式化表示

广义地说，形式化方法指有严格数学基础的系统开发方法，支持计算机系统及软件的规约、设计、验证与演化等活动。

在需求阶段引入形式化方法，可以将系统的形式化验证提前到需求规约阶段，从而达到尽早发现错误，降低错误修改代价的目的。

在需求阶段进行形式化验证，需要：

（1）确定（需要构建的系统的）系统模型；

（2）确定系统需要满足的性质；

（3）选择合适的验证工具。系统需要满足的性质，就是我们需要验证的性质，由性质规约语言描述，这些性质刻画所期望的系统行为。验证工具承载了验证技术，包括模型检测和定理证明。

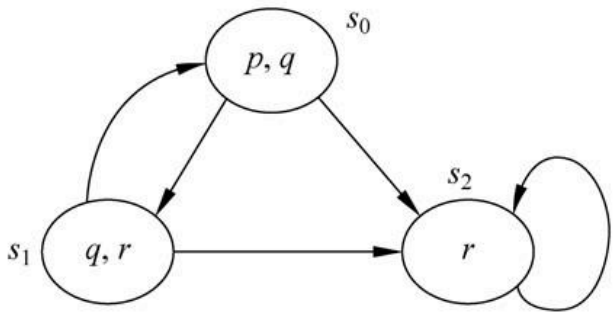
需求形式化建模

状态迁移系统(State Transition Systems)是一种基于状态迁移的计算模型，即通过状态（静态结构）和迁移（动态结构）来建模系统行为。它可定义为一个六元组：

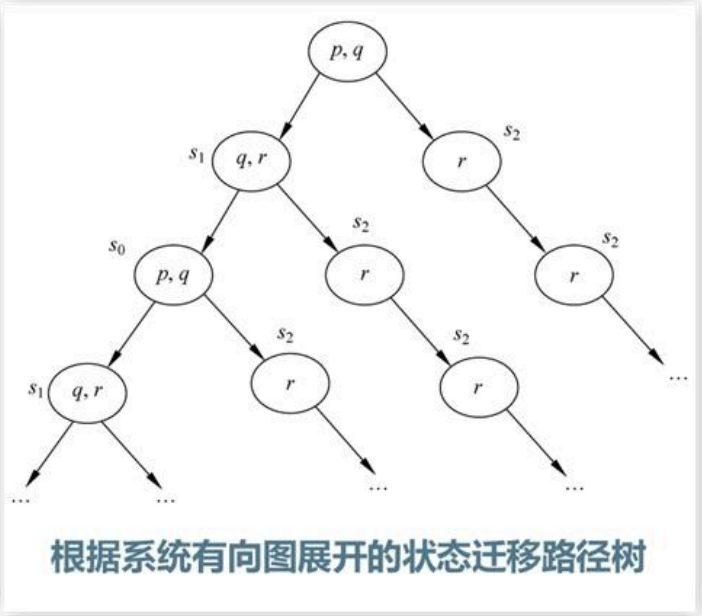
$$M:=(S,Act,\rightarrow,I,AP,L)\ ,$$

其中，S是状态集，包含系统可以处于的所有状态，Act是行为集，包含可以发生的所有事件，$\rightarrow\ \subseteq S\times Act\times S$是迁移函数，$I\subseteq S$ 是初始状态集，AP是命题集，$L:S\rightarrow 2^{AP}$是标签函数，表示如果系统处于某个状态，则有和该状态关联的一组命题为真。

状态迁移系统-图形表示



迁移系统作为有向图的简明表示



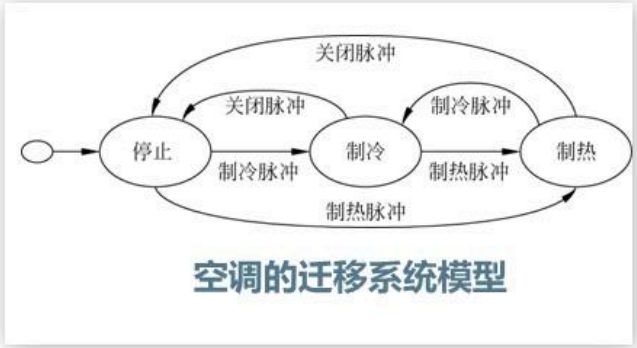
根据系统有向图展开的状态迁移路径树

例如，假设存在一个状态迁移系统，它有三个状态s_0、s_1和s_2，初始状态为s_0，状态间的迁移有$s_0 \rightarrow s_1$，$s_0 \rightarrow s_2$，$s_1 \rightarrow s_0$，$s_1 \rightarrow s_2$和$s_2 \rightarrow s_2$，若有$L(s_0)=\{p,q\}$,$L(s_1)=\{q,r\}$，$L(s_2)=\{r\}$

状态迁移系统的行为解释为： 从初始状态$s_0 \in I$开始，根据当前发生的事件，以及迁移关系→，决定系统状态的演化过程。具体地说，如果系统的当前状态为s，当事件α发生时，则系统不确定地选择迁移关系 $s \rightarrow (a) s'$(即 $(s,\alpha,s') \in \rightarrow$)，并将当前状态从s演化为s'。在当前状态为 s'的时候重复这个过程，**直到系统处于某个没有可迁移的状态，则状态演化结束。**

状态迁移系统例子

空调的状态变迁系统



空调的迁移系统模型

其中，椭圆代表状态，**带标记的边代表状态迁移关系，空心椭圆指向的状态为初始状态。**

这里，状态集合S={停止,制冷,制热}。初始状态集合只有一个状态，即I={停止}。“关闭脉冲”表示关空调的信号，“制热脉冲”表示让空调制热的信号，“制冷脉冲”表示让空调制冷的信号，因此Act={关闭脉冲,制热脉冲,制冷脉冲}。带标记的边是空调的状态变迁关系，例如，“停止制冷脉冲制冷”表示当空调处于“停止”状态时，收到“制冷脉冲”信号，则空调进入“制冷”状态。

空调要满足的原子命题可以完全和其状态的含义一致，即对任意状态s，有L(s)={s}。例如L(停止)={停止}，这是一种最简单的情况，即在状态命名的时候能找到和所关注的现实世界性质完全一致的状态名。

需求的状态迁移系统表示

- **首先考虑状态的选取**，系统状态的选取跟建模的目的直接相关，对于同一个系统，建模的目的不同，其状态的选取也会不同。例如，同样是一盏灯，如果只关心灯亮还是不亮，则会将“灯亮”作为一个状态，“灯灭”作为另一个状态； 而如果关心的是灯的亮度是不是适合学习，则假设灯的照度在300~500勒克斯时适合学习，为“亮度适合”状态，照度小于300勒克斯为“亮度偏弱”状态，照度大于500勒克斯作为“亮度偏强”状态。
- 除了状态集合，**还必须描述状态之间的迁移关系**。状态间的迁移关系通常可以这样确定： 从任意一个状态出发，考虑该系统是否可能从这个状态直接变化为其他某个状态，如果可能，则需要进一步确定能触发这个变化的事件，这就确定了该系统的一个状态迁移关系。例如，对于上述仅关心灯亮还是不亮的情形，当灯处于“灯亮”的状态时，收到“关脉冲”，则变为“灯灭”状态； 而当灯处于“灯灭”的状态时，收到“开脉冲”，则变为“灯亮”状态。
- **最后要确定原子命题集合AP，以描述所关注的物理世界情形和系统状态间的对应关系**，即确定一组关于现实世界的原子命题，将它们作为系统状态选择的依据，反过来说，原子命题就是系统处于某个状态所能确定为真的关于现实世界事实的命题。如上述例子中，系统处于“亮度偏弱”状态则意味着当前照度小于300勒克斯，处于“亮度偏强”状态则意味着当前照度大于500勒克斯。如果原子命题只在一个系统状态下满足，也可以直接将原子命题作为状态名，即对任意状态s，L(s)={s}，如上述将灯亮这个现实世界命题对应于“灯亮”状态，将灯不亮这个现实世界命题对应于“灯灭”状态。

性质规约语言简介

性质规约语言以时态逻辑为基础。时态逻辑有很多种，本节介绍常用的线性时态逻辑和计算树逻辑。

(1) 线性时态逻辑(Linear Temporal Logic，LTL)

线性时态逻辑将时间建模成状态的序列，无限延伸到未来。这个状态序列有时称为计算路径(简称路径)。一般来说，未来是不确定的，因此考虑若干路径，代表未来的不同可能，任何一条都可能是未来的“实际”路径。

线性时态逻辑的基本成分包括： 关于现实世界情形的原子命题(a∈AP)，布尔连接子（如∧），以及两个基本的时态算子O(下一个状态)和U(直到)。其中，原子命题(a∈AP)直接和状态变迁系统的相关联，时态算子为一元前缀算子，其参量为一个LTL公式，其含义是： 公式Oφ在当前时刻成立，则φ在下一时刻成立。U 时态算子为二元时态算子，带两个LTL 公式作为其参量，φ1Uφ2在当前时刻成立，则φ1一直成立直到在未来某个时刻φ2成立。

LTL的语法定义如下。

定义 原子命题公式集AP上的LTL公式由如下语法构成

其中，a∈AP为原子公式。 $\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid O\varphi \mid \varphi_1 U \varphi_2$

性质规约语言简介

(2) 计算树逻辑(Computational Tree Logic，CTL)

计算树逻辑是一种分支时间逻辑，它的时间模型是一个树状结构，表明未来是不确定的。在未来的不同路径中的任何一条都可能是“实际”路径。

定义9.2原子命题公式集AP上的CTL公式由如下语法构成：

$$\Phi ::= \text{true} \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg \Phi \mid \exists \varphi \mid \forall \varphi$$

$$\varphi ::= O\Phi \mid \Phi_1 U \Phi_2$$

其中，a∈AP为原子公式，φ是路径公式，Φ、Φ1和Φ2是状态公式。状态公式中的两个带量词的公式分别表示“存在一条路径”和“对所有路径”。

有一些经常需要表达的性质，如下：

存在一个可达状态满足a。可以写为 $\exists O \exists O \cdots \exists O a$

从所有满足a的可达状态出发，可以连续保持a的可满足性，直到到达一个满足b的状态。可以写为 $\forall \Box (a \rightarrow \exists (a U b))$

如果满足a的状态可达，可以永远连续不断满足b。可以写为 $\forall \Box (a \rightarrow \exists (\text{true} U \Box b))$

存在一个可达状态，由其出发的所有可达状态都满足b。可以写为： $\forall \Box b$

性质的时态逻辑表示

时态逻辑公式

需求的通用性质和特定性质都要用时态逻辑公式表达出来，才能使用模型检测器进行验证。在需求模型验证中，要验证的性质基本上都转换为可达性或无死锁性，但具体怎么转换，不同模型检测器会有不同的方式，具体如何描述也依赖于所使用的语言和工具。

下面列举一些常见性质描述的例子。

（1） 安全性： 两列火车Train1和Train2绝不同时进入同一个轨道区段Track。

$$\Box(\neg \mathrm{Train}_1 \text{ in Track} \vee \neg \mathrm{Train}_2 \text{ in Track})$$

（2） 活性： 每列火车都能无限多次进入同一条轨道区段。

$$\Box\Diamond \text{ Train in Track}$$

（3） 弱活性： 每列等待的火车总能进入某个路段。

$$\Box\Diamond \text{Train waitfor Track} \rightarrow \Box\Diamond \text{Train in Track}$$

需求验证

验证技术：模型检测技术

需求验证中最常见的验证技术是模型检测。模型检测就是对模型的状态空间进行搜索，以确定该系统模型是否满足某些性质，搜索的可中止性依赖于模型的有限性。在模型检测中，模型M一般为迁移系统，性质Φ是时态逻辑公式，而验证过程就是计算模型M是否满足Φ，即：

$$M \models \Phi$$

需求工程中存在需求R、环境E和需求规约S三部分描述，它们之间存在E,S ⊨ R关系。根据待验证的模型和性质的表示，需求验证涉及如下几种类型的验证。

（1） 需求R满足通用性质Φ，Φ可以是一致性、完整性等性质： $R \models \Phi$

（2） 规约S满足通用性质Φ： $S \models \Phi$

（3） 实现规约S的软件部署到环境E中后满足通用性质Φ： $E,S \models \Phi$

（4） 实现规约S的软件部署到环境E后满足需求R： $E,S \models R$

模型检测工具

业界有很多模型检测工具，它们使用的模型规约语言都有一些不同，所支持的时态逻辑也不尽相同，所以在模型检测的过程中需要了解所采用的模型检测器的要求。下面是一些在需求阶段常用的模型检测器。

- UPPAAL(Uppsala University & Aalborg University)： 时间自动机的模型检测工具，用于建模和模拟及验证实时系统的工具，支持网络化时间自动机和数据类型以及概率模型检验。
- SMV(Symbolic Model Verifier)： 符号模型检测器，用来检测有限状态系统是否满足CTL公式。
- NuSMV(New Symbolic Model Verifier)： 新符号模型检测工具，重构了SMV，支持用CTL和LTL描述，整合了以SAT为基础的有界模型检测技术。
- SPIN(Simple Promela Interpreter)： 适用于验证并发系统，用以检测有限状态系统是否满足PLTL（Propositional Linear Temporal Logic,命题线性时序逻辑）公式及其他一些性质，包括可达性和循环。建模语言为PROMELA(PROcess MEta LAnguage)。
- MyCCSL： 基于约束求解器Z3的有界模型检测器，用于支持实时和嵌入式系统的建模和分析，其输入语言为时钟约束规范语言（CCSL），可以建模时钟之间的关系，提供处理逻辑时钟的具体语法。

案例研究

NuSMV简介

本节采用NuSMV作为模型检测器，SMV作为模型规约语言，CTL作为性质规约语言。

NuSMV简介

NuSMV(New Symbolic Model Verifier)针对有限状态自动机系统提供模型检测能力，支持CTL和LTL描述的性质规约。NuSMV程序由一个或多个模块构成，其中有一个主模块(main)。模块可以声明变量并赋值，赋值通常给出变量的初始值(initial)，其随后值(next)是关于变量当前值的表达式。LTL(或CTL)规范由关键词LTLSPEC(或者CTLSPEC)引入。为了方便表示，NuSMV分别用标准键盘上的&、|、→、!、F、G、E和A来分别表示∧、∨、→、◇、□、¬、∃和∀。

```
MODULE main
VAR
        request: boolean;
        state :{ready,busy};
ASSIGN
      init(state) :=ready;
      next(state) := case
                request = 1 & state = ready : busy;
                TRUE: ready;
         esac;
LTLSPEC
      G(request->F state=busy)
```

NuSMV程序举例

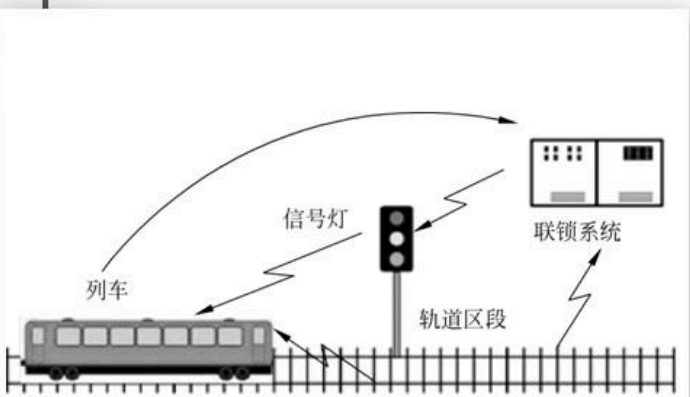
右图给出NuSMV程序本章中的NuSMV工具采用其2.6.0版本。的例子，该程序有两个变量，布尔(boolean)型的request和枚举型{ready,busy}的state，其中0代表“假”，1代表“真”。变量request的初始值和随后值在这个程序中不确定，表明它的取值是由外部环境决定的。state的初值是ready，当request为1且state为ready时变为busy，否则(即文中的TRUE)state的随后值为ready。待验证的性质描述为LTLSPEC，表示一旦有request，则未来state会变成busy。

案例研究

简化的轨道交通联锁系统

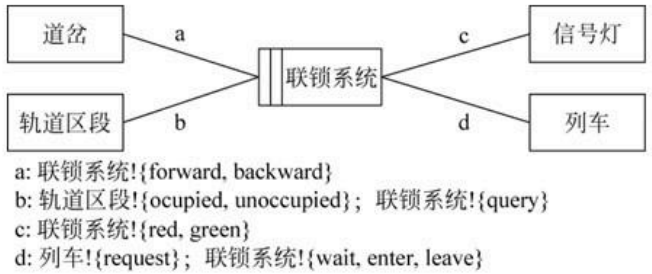
在轨道交通系统中，联锁系统是其信号系统的核心设备，用于保证列车行车安全。铁路、地铁车站及车辆段都有很多线路，线路的两端以道岔连接，根据道岔的不同位置组成列车的不同进路，每条进路只允许一辆列车使用。列车能否进入某进路，如何避免发生进路冲突，这些都由联锁系统来协调。通常，一个铁路编组站由四类组件构成：轨道区段、道岔、进路和信号灯。联锁系统的主要功能包括轨道区段的分配、进路控制、道岔控制、信号控制等。

一个轨道交通联锁系统的简化场景如下：**一辆列车(train，含车载系统)在进入轨道之前需要向联锁系统(controller)发出请求。**controller查询轨道的占用状态，决定是否接受其请求。若列车收到红灯信号，则列车等待并重复发送请求；若收到绿灯信号，则列车等待道岔打开，进入相应的进路。右图给出了轨道交通联锁系统的示意图。



轨道交通联锁系统示意图

系统模型构建



联锁系统的上下文图

第一步：结构建模

确定系统的组件及这些组件之间的交互关系，可以用上下文图表示。

针对这个简化的联锁系统(controller)，可以识别出该系统有4个环境实体： 轨道区段(track)、道岔(switch)、列车(train)和信号灯(light)。其中，轨道区段在占用状态和未占用状态之间来回转换，道岔在正向与反向状态之间来回转换，信号灯在红灯与绿灯之间转换，列车在发送请求之后需要经历从等待、进入到离开的过程。

系统模型构建

第二步：组件建模

上述的组件识别过程已经大致确定了每个组件的行为。

例如，联锁系统的行为如下：收到列车的请求之后，查看轨道状态，若其当前状态为“占用”，则给信号灯发出红灯脉冲，指示信号灯进入“红灯”状态，达到让列车等待的目的。联锁系统按照一定的时间频率接收列车的请求，若发现轨道状态为“未占用”，则给信号灯发出绿灯脉冲，指示信号灯进入“绿灯”状态，达到通知列车可以进入轨道的目的，同时控制道岔，让列车进入。之后联锁系统处于空闲状态，等待下一次列车的请求信号。

以上述行为分析的结果为依据，定义各组件的状态。首先考虑各组件的可能状态。

- 对信号灯而言，有红灯(red)和绿灯(green)两个状态；
- 对轨道区段而言，有未占用(unoccupied)和占用(occupied)两个状态；
- 道岔因为有正向和反向两种情况，有正向(forward)和反向(backward)两个状态，假设反向为允许进入；
- 列车有请求已发送(requested)、等待(wait)、进入(enter)和离开(leave)四个状态；
- 系统的状态包括：已接收请求(receiveRequest)、轨道查询(queryTrack)、已发送等待(sendWait)、已发送进入(sendEnter)和空闲(idle)。

然后，分别定义初始状态。

- 信号灯的初始状态为red，轨道区段为unoccupied，列车为requested，道岔为forward，联锁系统为idle。

第三步：定义求随后状态的函数

（1） next(controller):

如果controller处于idle或sendWait状态且列车处于requested状态，则函数值为receiveRequest；如果controller处于receiveRequest状态，则函数值为queryTrack；

如果controller处于queryTrack状态且轨道处于unoccupied状态，则函数值为sendEnter； 如果controller处于queryTrack状态且轨道处于occupied状态，则函数值为sendWait；

如果controller处于sendEnter状态且列车处于enter状态，则函数值为idle； 其他情况下函数值不变。

（2） next(light):

如果light处于red状态，controller处于sendEnter状态且train处于requested状态，则函数值为green； 其他情况下函数值为red。

（3） next(train):

如果train处于requested状态，light处于green状态且switch处于forward状态，则函数值为enter； 如果train处于requested状态，且controller处于sendWait状态，则函数值为wait； 如果train处于enter状态,且track处于occupied状态，则函数值为leave； 如果train处于leave状态或wait状态，则函数值为requested； 其他情况下函数值不变。

（4） next(track):

如果track处于unoccupied状态，且train处于enter状态，则函数值为occupied； 如果track处于occupied状态，且train处于leave状态，则函数值为unoccupied；

其他情况下函数值不变。

（5） next(switch):

如果switch处于forward状态，且controller处于sendEnter状态，则函数值为backward； 其他情况下函数值为forward。

最后，得到联锁系统的SMV模型，如右图所示。

```
MODULE main
VAR
light : {green,red};
track : {occupied,unoccupied};
switch : {forward,backward};
train : {requested,wait,enter,leave};
controller : {receiveRequest,sendWait,queryTrack,sendEnter,idle};
ASSIGN
init(light) := red;
init(track) := unoccupied;
init(switch) := forward;
init(train) := requested;
init(controller) := idle;
next(controller) := case
        (controller=idle|controller=sendWait) &train=requested : receiveRequest;
        controller=receiveRequest : queryTrack;
        controller=queryTrack & track=unoccupied : sendEnter;
        controller=queryTrack & track=occupied : sendWait;
        controller=sendEnter & track=enter : idle;
        TRUE : controller;
    esac;
next(light) := case
        light=red&controller=sendEnter & train=requested: green;
        TRUE : red;
    esac;
next(train) := case
        train=requested & light=green & switch=forward : enter;
        train=requested & controller=sendWait : wait;
        train=enter & track=occupied : leave;
        train=leave | train=wait : requested;
        TRUE : train;
    esac;
next(track) := case
        track=unoccupied&train=enter : occupied;
        track=occupied&train=leave : unoccupied;
        TRUE: track;
    esac;
next(switch) := case
        switch =forward & controller=sendEnter : backward;
        TRUE: forward;
    esac;
```

联锁系统的NuSMV程序

验证性质

（1） 一致性： 无冲突。

要求联锁系统的需求是一致的，即没有冲突需求。可以表示为在任何情况下，都不可能出现同一组件处于两个不同的状态。

AG!((light=green & light=red)|(track=occupied & track=unoccupied)|(switch=forward & switch=backward)|(train=requested & train=wait)|(train=requested & train=enter)|(train=requested & train=leave)|(train=wait & train=enter)|(train=wait & train=leave)|(train=enter & train=leave)|(controller=idle & controller=receiveRequest)|(controller=idle & controller=queryTrack)|(controller=idle & controller=sendWait)| (controller=idle & controller=sendEnter) |(controller=receiveRequest & controller=queryTrack)|(controller=receiveRequest & controller=sendWait)|(controller=receiveRequest & controller=sendEnter)|(controller=queryTrack & controller=sendWait)|(controller=queryTrack & controller=sendEnter)|(controller=sendWait & controller=sendEnter))

(2) 领域特定的性质： 绿灯，则车辆进入； 红灯，则车辆不能进。

需求可满足性，需求可以表示为如绿灯则列车进入，红灯则列车不能进站等。

AG (light=green AF train=enter)

AG (light=red AF (train!=enter))

将模型与性质输入NuSMV验证器中，即可验证这些性质都是可满足的。

思考题

1. 需求阶段一般需要验证哪些性质?

2. 假设一个系统的描述中有如下原子命题：忙(busy)、开始(started)、准备好(ready)、确认(acknowledged)、重启(restart)和请求(request)。如何用时态逻辑描述如下性质?

不可能到达一个started成立但ready不成立的状态;

可能到达一个started成立但ready不成立的状态:

对任何状态，如果一个(对某些资源的)request发生，那么它将最终被acknowledged;

不管发生什么情况，一个特定过程最终被永久死锁(deadlock);

从任何状态出发都可能到达一个restart状态。

3. 请使用NuSMV对如下案例进行建模和验证。

地铁屏蔽门控制系统就是控制站台屏蔽门的开关。当列车到站并停在允许的误差范围内时(如±300mm)，信号系统将向屏蔽门控制系统发送开门指令，打开屏蔽门。当列车驾驶员或站务人员通过就地控制盘发出关门命令时，系统关闭站台屏蔽门。

4. 请选择合适的形式化语言对如下机房自动温度控制系统进行建模，并进行性质的验证。

机房服务器持续运作会导致机房温度过高，产生安全隐患，需要设计一套机房温度自动控制系统来解决这个问题。假设在一个密闭的机房中放置一台服务器、一台空调和一个温度传感器，服务器持续工作会带来房间热量的增加，温度传感器负责检测温度并对空调发出信号，空调负责制冷降温。当机房的温度超过30℃时，将打开空调；当机房的温度低于20℃时，关闭空调。

参考文献

[1] European Committee for Electrotechnical Standardization.BS EN 50129: Railway application Communications,signaling and processing systems—Safety related electronic systems for signaling [EB/OL] .(2019 05 13) [2022 12 05] .https://www.en standard.eu/bs en 50129 2018 railway applications communication signalling and processing systems safety related electronic systems for si gnalling/.

[2] RTCA. DO 178C Software Considerations in Airborne Systems and Equipment Certification [M] .Washington, USA: RTCA Inc.,2011.

[3] Yuan Z,Chen X,Liu J, et al.Simplifying the Formal Verification of Safety Requirements in Zone Controllers through Problem Frames and Constraints Based Projection [J] .IEEE Transactions on Intelligent Transportation System, 2018,19(11): 3517 3528.

[4] 刘筱珊,袁正恒,陈小红,等.区域控制器的安全需求建模与自动验证 [J] .软件学报,2020,31(5): 1374 1391.

[5] Chen X,Wu X,Zhao M,et al.Verifying the Relationship Among Three Descriptions in Problem Frames Using CSP [C] //TASE 2019: 248 255.

[6] Baier C,Katoen J.Principles of Model Checking [M] .Cambridge,MA: MIT Press,2008.

[7] Liu S.Formal Engineering for Industrial Software Development [M] .Berlin: Springer,2004.

[8] Aceituna D,Do H,Srinivasan S.A Systematic Approach to Transforming System Requirements into Model Checking Specifications [C] //ICSE Companion 2014: 165 174.

[9] Bultan T,Heitmeyer C.Analyzing Tabular Requirements Specifications Using Infinite State Model Checking [C] //MEMOCODE 2006: 7 16.

[10] Shrotri U,Bhaduri P,Venkatesh R.Model Checking Visual Specification of Requirements [C] //SEFM 2003: 202 209.

[11] Choi Y,Rayadurgam S,Heimdahl M.Toward Automation for Model Checking Requirements Specifications with Numeric Constraints [J] .Requirement Engineering,2002,7(4): 225 242.

[12] Fuxman A,Mylopoulos J,Pistore M,et al.Model Checking Early Requirements Specifications in Tropos [C] //RE 2001: 174 181.

[13] Bharadwaj R,Heitmeyer C.Model Checking Complete Requirements Specifications Using Abstraction [J] .Automated Software Engineering,1999,6(1): 37 68.

[14] Heitmeyer C,Kirby J,Labaw B,et al.Using Abstraction and Model Checking to Detect Safety Violations in Requirements Specifications [J] .IEEE Transactions on Software Engineering,1998,24(11): 927 948.

[15] Clarke E,Henzinger T,Veith H,et al(eds).Handbook of Model Checking [M] .Cham,Switzerland: Springer International Publishing AG,2018.

[16] 王戟,詹乃军,冯新宇,等.形式化方法概貌 [J] .软件学报,2019,30(1): 33 61.

[17] Heitmeyer C,Jeffords R,Labaw B.Automated Consistency Checking of Requirements Specifications [J] .ACM Transactions on Software Engineering and Methodology,1996,5(3): 231 261.