北京交通大学
BEIJING JIAOTONG UNIVERSITY

基于扩展动态活动图的列控系统运行时验证

报告人：柴铭
chaiming@bjtu.edu.cn
北京交通大学

SAVE 2016




研究背景

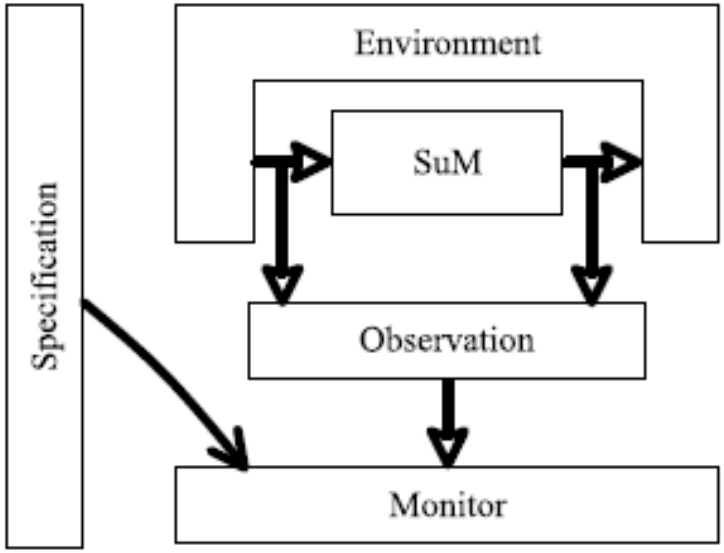
- 列控系统的复杂性使其正确性很难保证
- 模型检验：
  - 形式的、完备的
  - 精确的模型难以建立
- 软件测试：
  - 直接测试真实系统
  - 充分的测试环境难以获取
- 实施与系统开发阶段

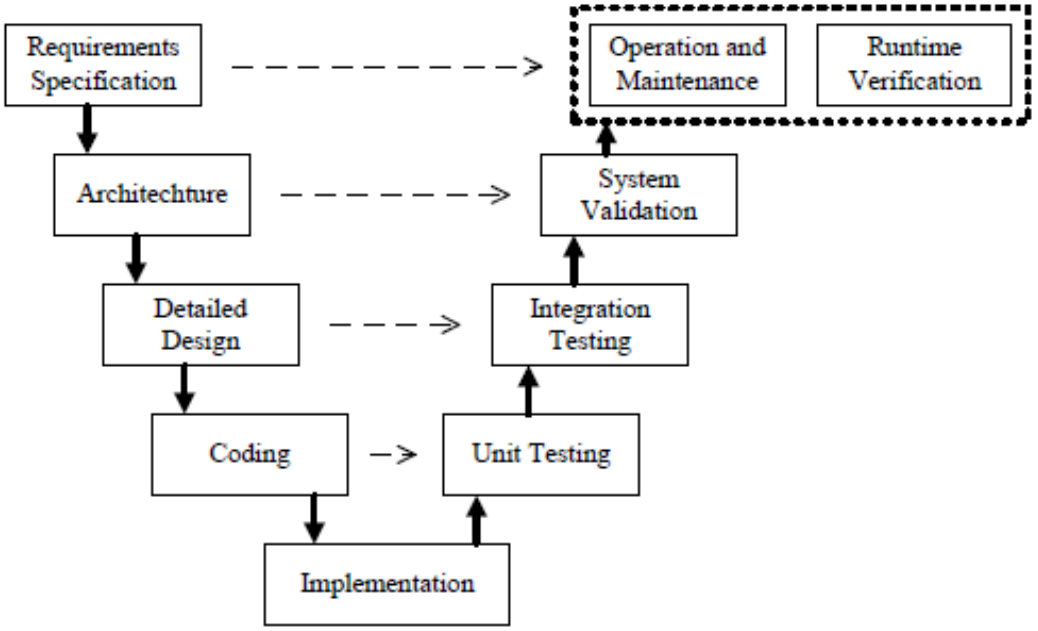
运行时验证

- 观测一个运行中的系统，并检查其是否满足期望的性质。
- 与模型检验相比：无需建立系统模型（直接观测真实系统）
- 与测试相比：无需人工建立环境（系统运行于真实的环境中）
- 利用“监控器”实施
  - 观测不改变系统的行为
  - 例外：中断或终止系统的执行

运行时验证

- 规范与监控之间的博弈：观测结果是否满足监控规范？
  - 监控规范：期望系统满足的性质
  - 观测结果：被监控器观测到的系统执行
  - 有限状态自动机的词问题



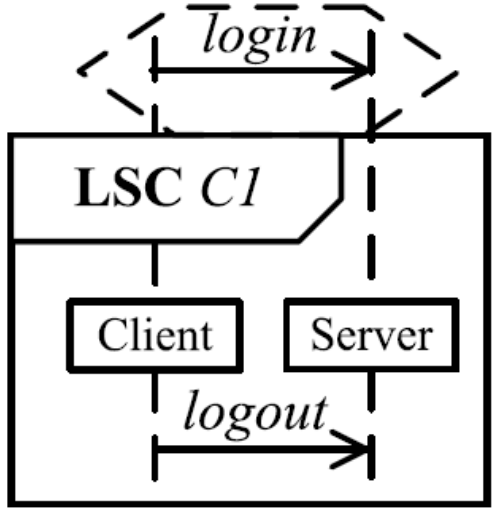


监控规范

- 挑战：建立具备美观性（**attractiveness**）和达意性（**expressiveness**）的监控规范语言。
- 文本化形式语言：例如LTL及其扩赞
  - 不具备美观性
- 图形化语言：例如消息序列图、UML
  - 不具备达意性

活动序列图（Live Sequence Chart）

- 活动序列图（LSC，由Damm 和 Harel提出）是消息图的模态扩展
- 全局图（**universal chart**）：描述了强制性行为，由两个基本图前图（prechart）和主图（main chart）组成
- 存在图（**existential chart**）：描述了可能的行为。



LSC的扩展

- LSC无法描述否定以及参数化性质
- 扩展LSC引入了模态前图：
  - 充分前图：主图的充分条件
  - 必要前图：主图的必要条件
- 参数化扩展LSC引入赋值结构和条件结构：
  - 赋值结构储存任意参数值
  - 条件结构描述参数值的约束

基本图的语法

- 每条消息存在两个事件：发送消息的事件和接收消息的事件
- 生命线：有限事件序列
- 基本图：n元生命线
- 事件发生：事件及其位置构成的三元组
- 通信：两个事件发生构成的对，这两个事件分别表示发送和接收同一条消息

基本图的语义

- 基本图引入了事件之间的偏序关系：
  - 在同一条生命线中，位置较高的事件发生先于位置较低的事件；
  - 对于一条消息，发生消息事件先于接收消息事件
- 一条迹被基本图接收 的充要条件为：
  - 每个事件仅发生一次
  - 事件的发生顺序满足基本图引入的偏序关系
  - 空言事件序列允许出现在任意两个事件之间
- 基本图的语言为所有被该图接收的迹的集合

扩展LSC的定义

- 扩展LSC（eLSC）为一个三元组

  $Uch = (p, m, Cate)$，其中p，m分别代表前图和主图，$Cate = (Nec, Suff)$

- $(p, m, Suff)$的语言为

$$\overline{\Sigma^* \circ L(p) \circ \overline{L(m) \circ \Sigma^*}}$$

- (p, m, Nec) 的语言为

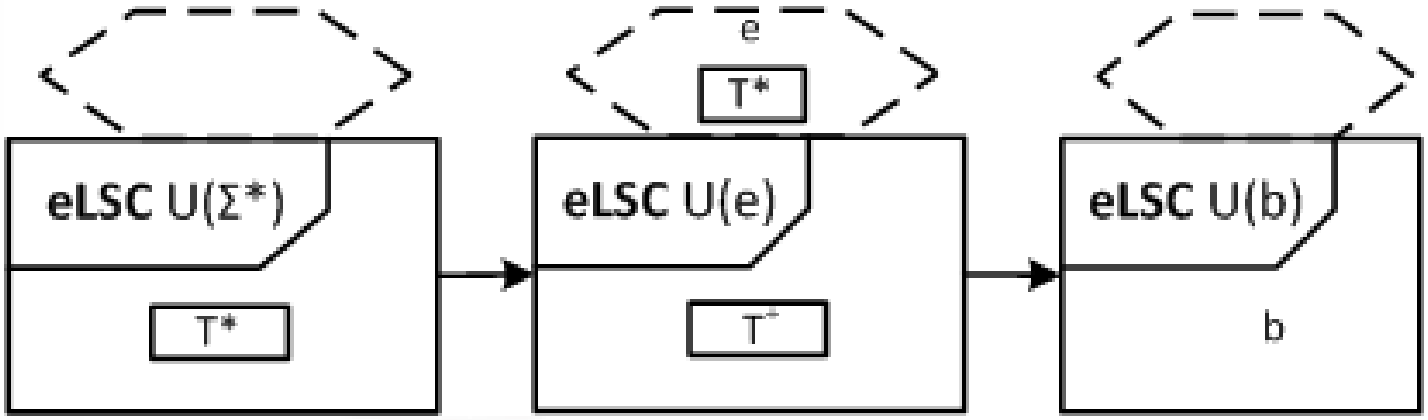
$$\overline{\overline{\Sigma^* \circ L(p)} \circ L(m) \circ \Sigma^*}$$

- eLSC的串接：

$$\mathrm{Uch}_1 \rightarrow Uch_2 = L(Uch_1) \circ L(Uch_2)$$

扩展LSC的表达能力

- 无空言eLSC：不包含空言事件的eLSC
- eLSC的表达能力严格高于标准LSC
- eLSC规范（即eLSC集合）在否定上是闭合的
- eLSC的表达能力等同于star-free正则语言
- 举例：a **U** b



参数化扩展LSC

- 通过引入赋值结构和条件结构描述带参数的性质：

- 赋值结构： $assi = (v, s, o)$，

  条件结构：$cond = (prop, o)$

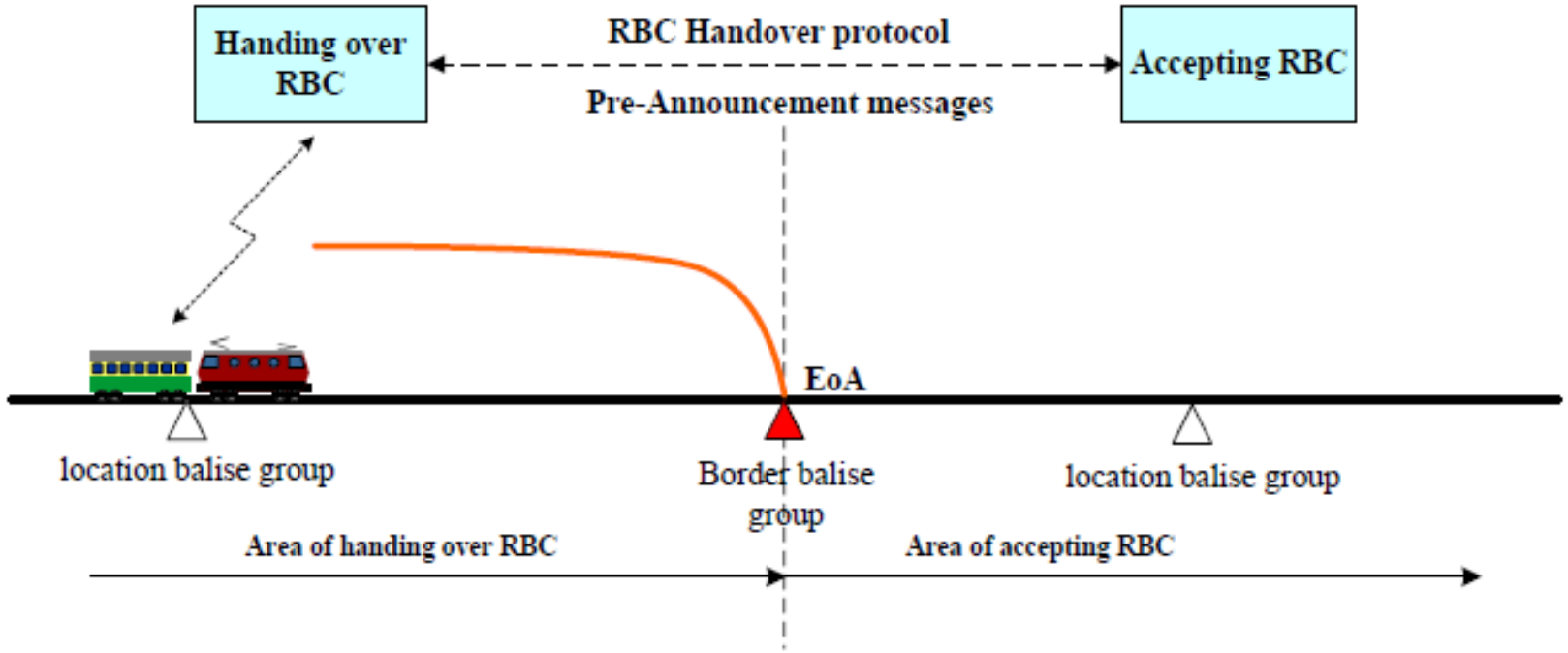
- 参数化扩展LSC（PeLSC）：

$PU = (Uch, COND, ASSI)$, 其中COND和 ASSI分别为赋值结构和条件结构的集合。

参数化扩展LSC的语义

- 参数： $p = (s, d)$ 由名字和取值组成的对
- 参数化事件： $w = (e, P)$ 由事件和参数集合组成的对
- 参数化事件迹： $\tau = w_1,\ldots w_n$ 由参数化事件组成的轨迹。
- 参数化事件迹被PeLSC接收的充要条件为：
  - （$e_1,\ldots e_n$）被Uch接收
  - 参数事件满足条件结构中的断言
  - 参数化空言事件迹可以出现在任意两个参数化事件之间

案例分析：RBC交接场景

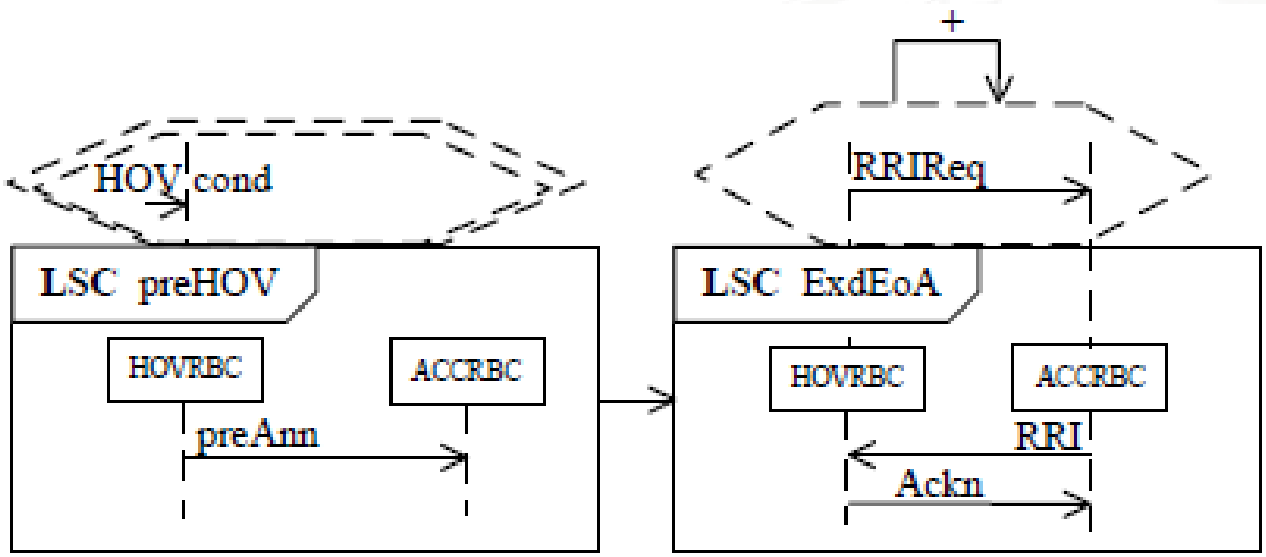


监控实现

- 监控过程分三步实现：
  - 利用eLSC和PeLSC描述文本化性质
  - 将eLSC和PeLSC分别转为LTL和HL
  - 利用LTL和HL的模型检验算法验证观察结构是否满足性质。

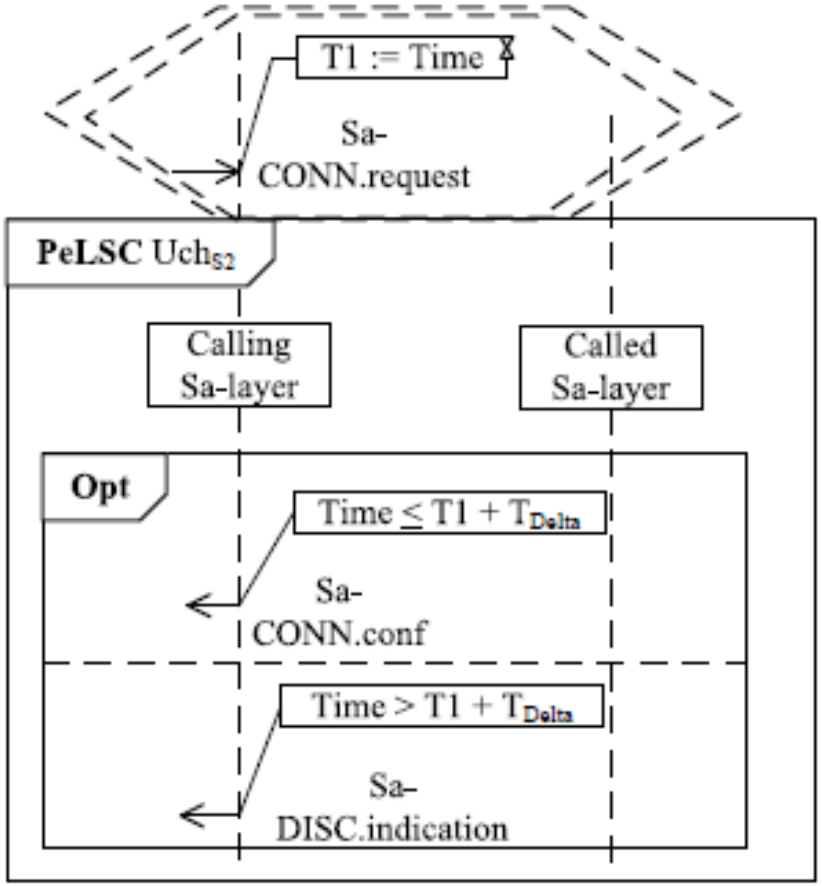
监控性质（eLSC）

- 如果列车到达移交预告点，则移交RBC和接收RBC交互NRBC消息



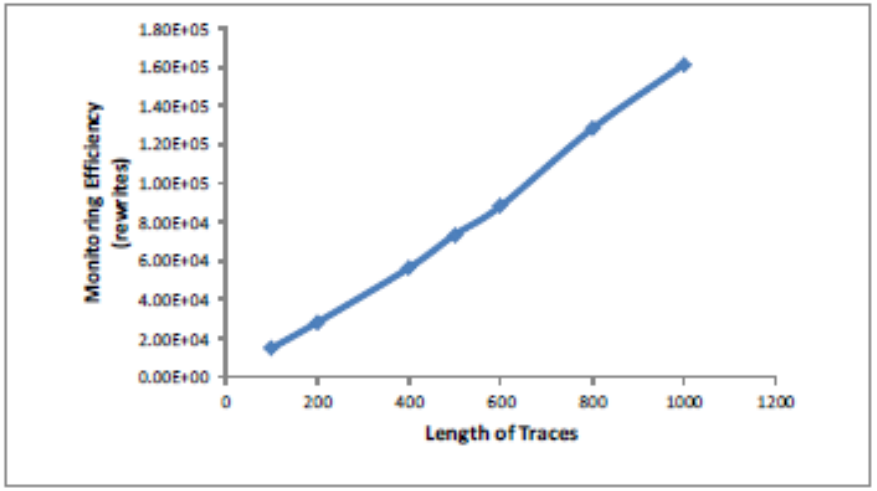
监控性质（PeLSC）

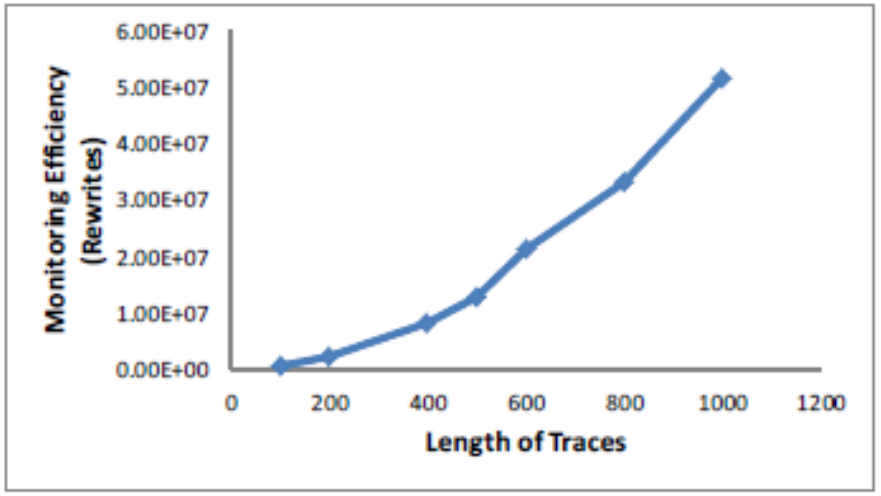
- 车载与接收RBC的安全连接应在一定时间内建立，否则提示通信未建立。



监控效率

- eLSC和PeLSC 的计算复杂度均为线性的。
- 在Maude中计算时间如下：





- 猜测：Maude中的某些计算规则使HL的复杂度为 $o(x^2)$

总结

- 运行时验证

  补充了模型检验和测试在复杂系统安全保障中的不足

- eLSC和PeLSCs:

  具备美观性和达意性的图形化形式语言，适用于规约监控规范

- 利用eLSC和PeLSC监控列控系统:

  将eLSC和PeLSC转换为LTL和HL进行监控是可行的，但还需要开发更加高效的算法。

谢谢！