

# 時間制約を含む連動図表のUPPAALによるモデル検査

(株)日立製作所

堀 悟

satoru.hori.fy@hitachi.com

## 開発における問題点

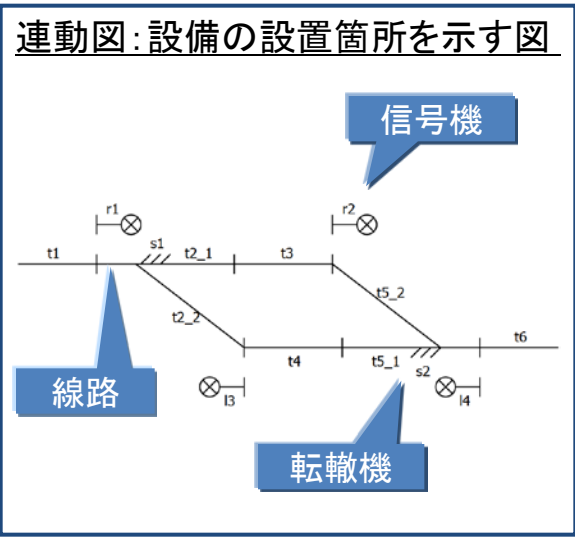
鉄道の運行管理システムにおいて、駅構内の列車運行を制御する信号機・転轍機の制御の仕様は連動図表と呼ばれる図と表によって記述されている。連動図表は比較的小さな駅でも複雑になり、設計・検査に要するコストや時間が大きいことが課題となっている。

## 手法・ツールの適用による解決

連動図表についてモデル検査により正しさを検証する。特に連動図表の時間制約に着目し、時間制約を表現できるモデル検査ツールであるUPPAALによるモデリング方法の提案と、連動図表からのUPPAALモデル生成ツールの試作を行う。

## 連動図表のモデル化・検証アプローチ

連動図表: 駅構内の列車運行を制御する信号機・転轍機\*の制御の仕様で、連動図と連動表により構成される  
 \*)列車の進路を制御する装置



**連動表: 信号機・転轍機の鎖錠\*の関係を示す表**  
 \*)信号機・転轍機を操作できないようにすること

名称	番号	鎖錠	信号制御またはつ查鎖錠	接近鎖錠
信号機	r1	s1	t2_1, t3	t1
...	...	...	...	...
転轍機	s1		t2_1, t2_2	...
...	...	...	...	...

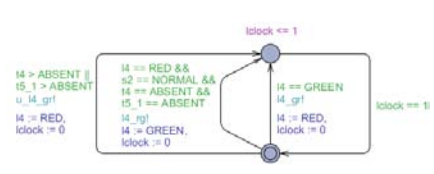
- 信号制御  
列車が存在するときに信号機を赤にする
- つ查鎖錠  
列車が存在するときに転轍機を転換できないようにする
- 接近鎖錠  
列車が接近しているときは、信号機が赤になってから一定時間経過するまで転轍機を転換できないようにする

UPPAALによりモデル化

ツール化し半自動生成

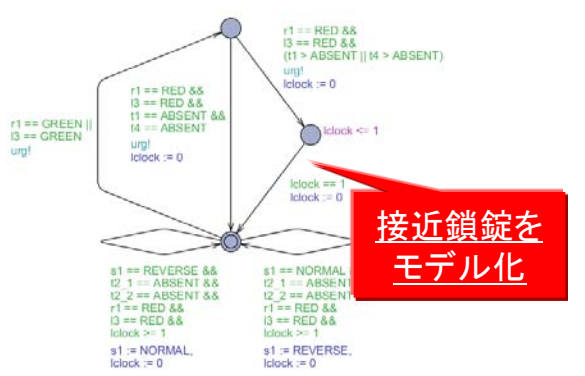
### 信号機

下の状態から上の状態に遷移する際に信号機の表示を変更する



### 転轍機

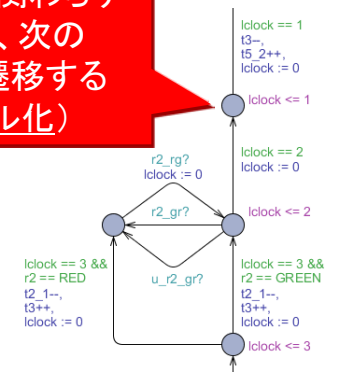
下の状態でのみ転轍機が転換可能  
列車接近中は転換可能状態に遷移する前に一定時間待機する



### 列車

青が2クロック続くと、その1クロック後に(赤でも)次の区間に遷移する

信号機の状態に関わらず1クロック後に、次の状態(区間)に遷移する(過走をモデル化)



列車が目的地に到達すること・衝突しないこと・脱線しないことを検証