STAMP/STPAとモデル検査との連携について —鉄道踏切「とりこ検知」例題をもとに—

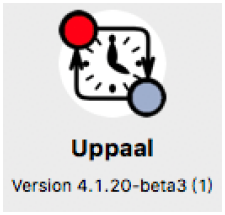
岡野 浩三† 楊 盼† 辛島 凜† 小形 真平†
†信州大学工学部

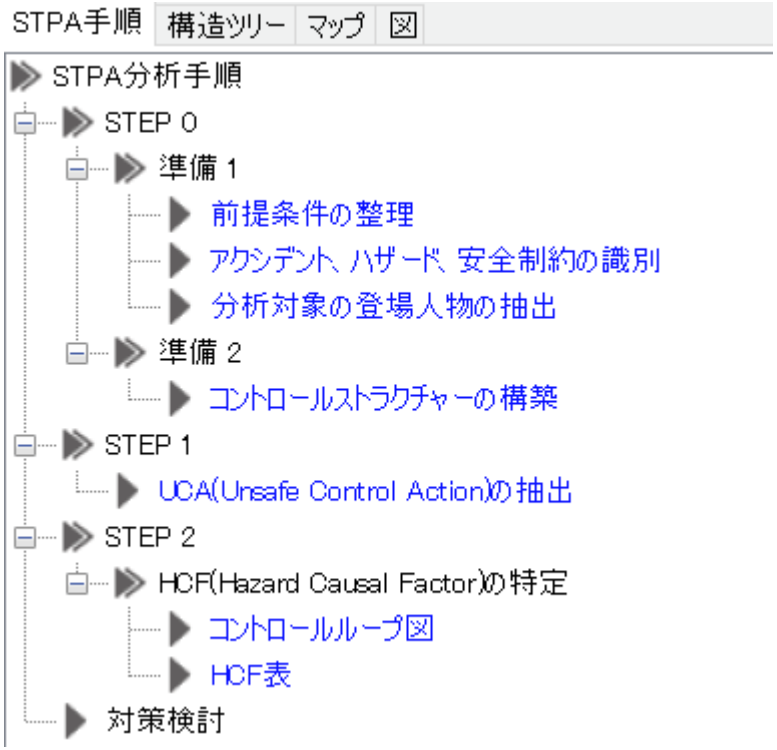
一部は仙台高専 岡本圭史氏との共同研究

STAMP Workbench

STAMP Workbenchは公開されている
STAMP/STPAを支援するツール[3]

STAMP Workbenchを使い、UPPAAL[4]との連携方法について考察を行う





[3] https://www.ipa.go.jp/sec/tools/stamp_workbench.html
[4] Johan Bengtsson and Wang Yi: “Timed automata: Semantics, algorithms and tools,” In Lecture Notes on Concurrency and Petri Nets, volume 3098, pp.87–124 (2004)

動機　問題意識

- STAMP/STPAでハザードシナリオが種々導出できる
- 人手の作業
- モデル検査の反例解析が応用できないか

これまでに

- 単線の踏切例題
- モデル検査
- シナリオ導出

内容

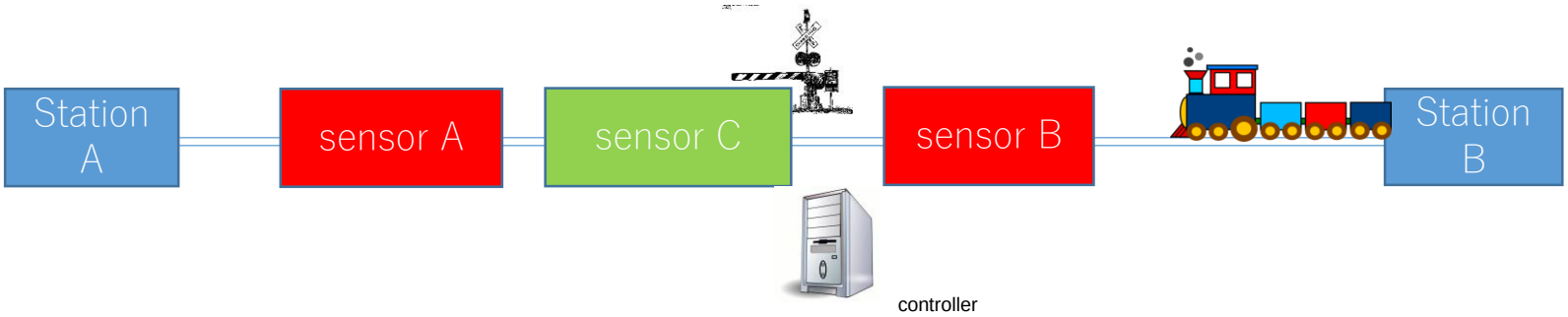
- これまでの取り組み１　　（単線踏切のモデル化モデル検証）
- これまでの取り組み２　　（とりこ検知）
- モデル検査との連携の観点からの考察
- 手法の提案 (WIP)

これまでの取り組み１

単線踏切

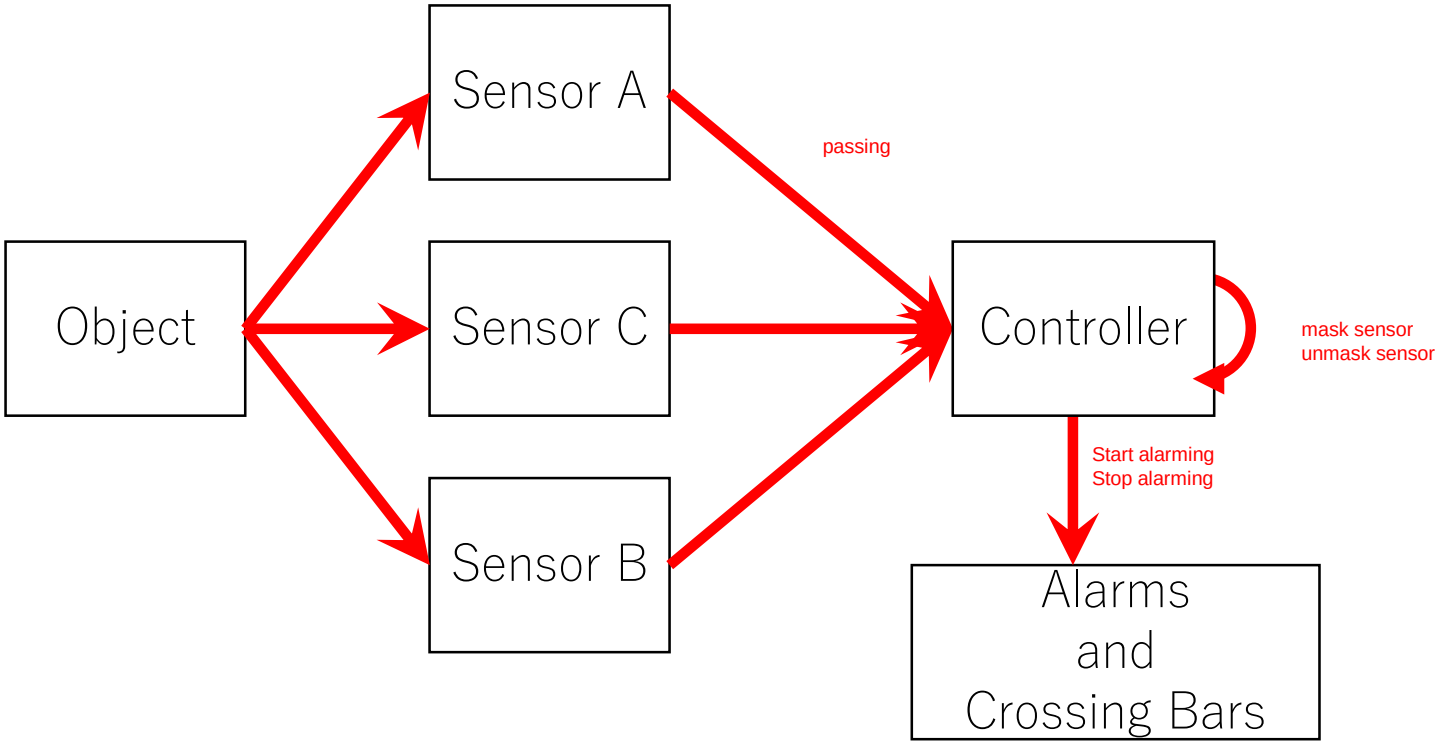
例題

- 単線踏切[2]



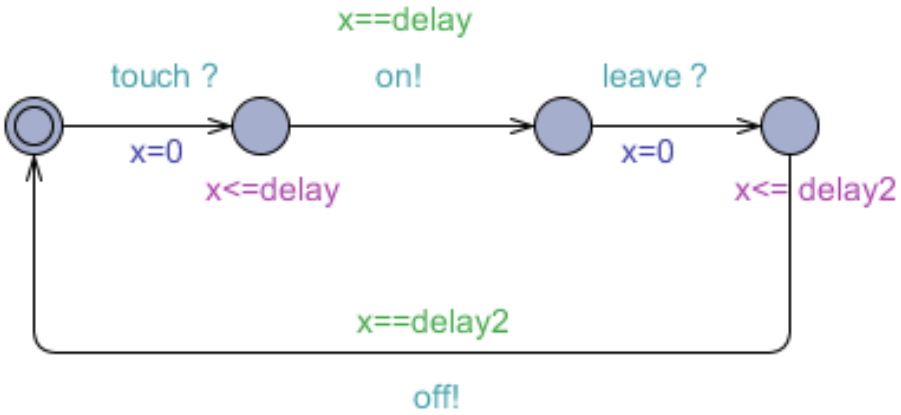
[2] システム安全性解析WG: “はじめてのSTAMP/STPA, 初級編”, 情報処理推進機構(2016)

Control Structure



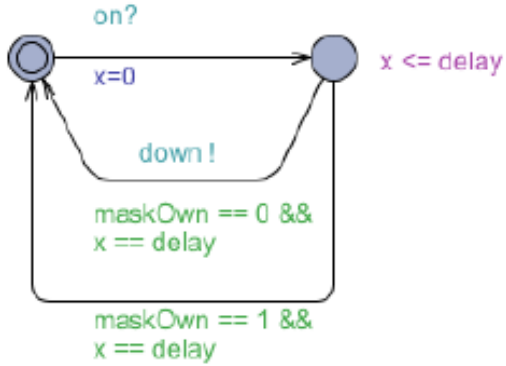
センサ A, B and C

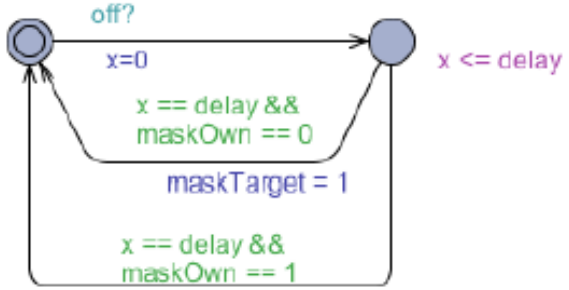
- 単純なモデル



コントローラ for センサ A and B

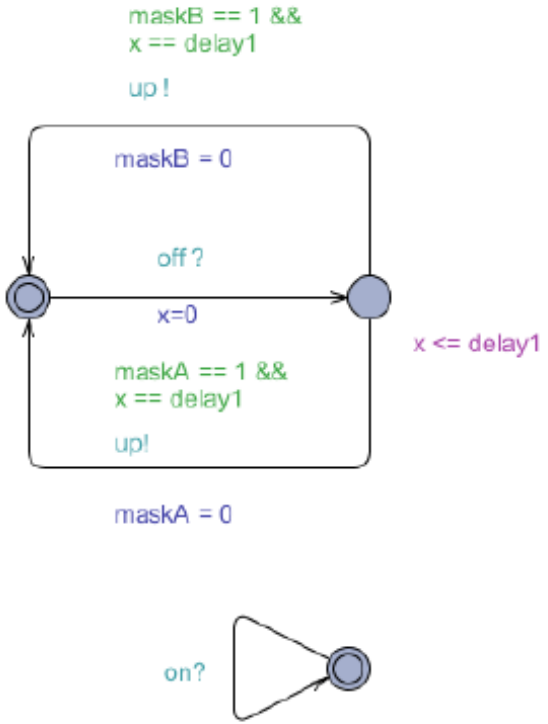
- maskの有無で動作場合分け
- on, off 信号個別にコントロール



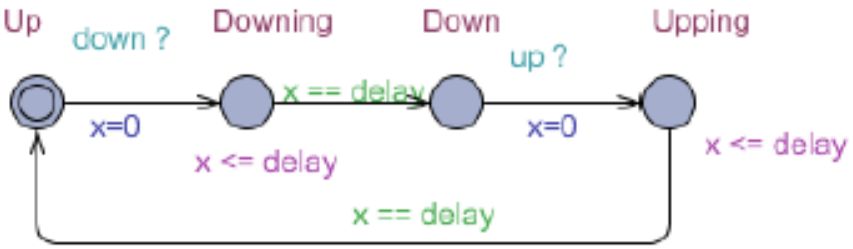


コントローラ for センサ C

- maskをしているセンサで場合分け
- On信号は原則無視



遮断機


Up
down ?
Downing
Down
up ?
Upping
x == delay
x=0
x=0
x <= delay
x <= delay
x == delay

試行1

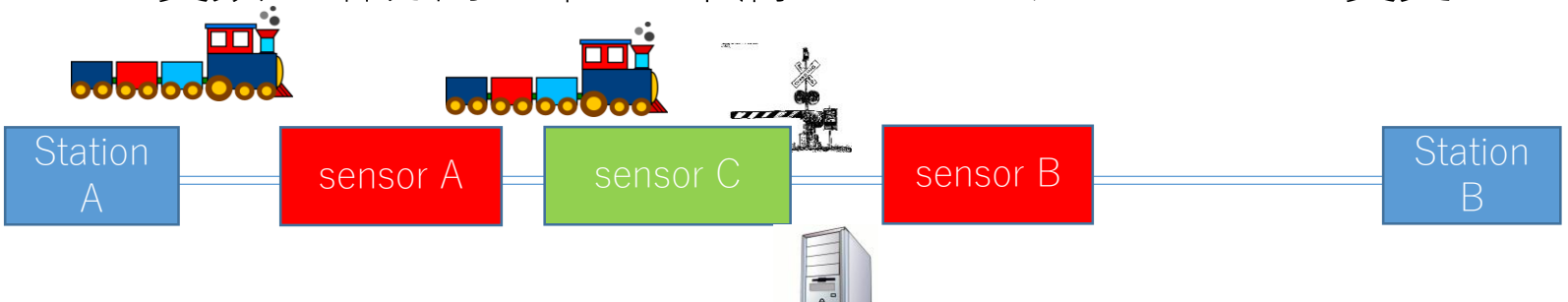
- Station AとStation Bを同一視し、1台の列車が常に左から右へ走り抜けるだけの動作を繰り返すモデル
- 全システムにたいして
  - deadlockのないことを確認
  - 各種時間パラメータを調整し、モデルを修正

試行2

- 列車を同一方向から2台動かす状況をモデル化

deadlock

- 踏切内に2台連続ではいることをシステムで想定していなかったことを意味する.
- 単線であることを考慮にいれ，踏切内にいる列車数の状態変数(セマフォ)を設ける
- この変数が踏切内で常に2未満になるようにモデルを変更



試行2

- このモデルで2台動かすシステムに対しては
  - deadlock
- にならないことを確認
  - $\mathbb{AG}(train.cs \Rightarrow db.down)$
- が不成立
- 反例を解析する
  - ちょうど1台目が踏切を出たところでまだ遮断機が下がっている状態で
  - 2台目が踏切内にはいると2台目が踏切内に入ってきたにもかかわらず，2台目に関わる踏切動作が(踏切の上昇動作中というタイミングにより)無視され
  - 遮断機があがることが起こり得る

試行2

- この「踏切の上昇動作中というタイミング」で制御信号を無視しない場合はシステムのデッドロックを引き起こすことが確認できており，このロジックはそう容易に改善できないと考えられる

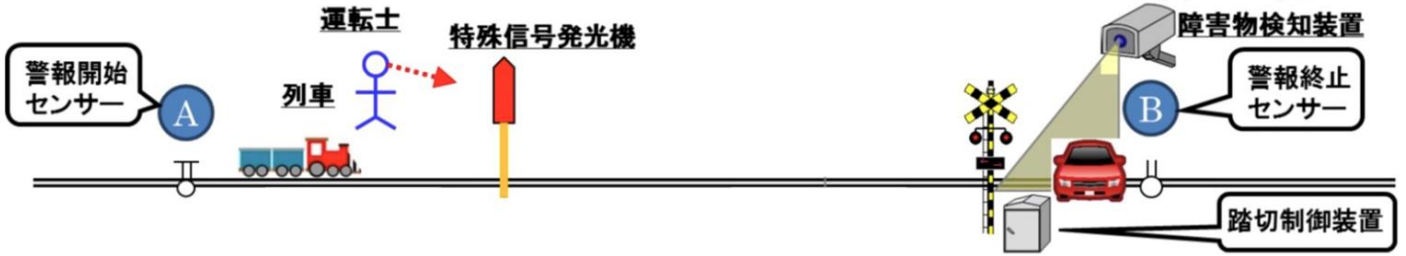
- このケースは文献[2]ではシナリオとして触れられていない

これまでの取り組み２

とりこ検知

例題

鉄道踏切「とりこ検知」[4]



文献[4]より

鉄道踏切において，遮断機が下りる状態で人あるいは車があるとき，接近中の列車に伝えて衝突を回避する.

- 列車の接近を警報開始センサーで検知して，踏切制御装置が踏切遮断機に遮断開始と障害物検知装置に検知開始を指示
- 障害物検知装置は踏切内に通行車・人があるか否か検知し，検知すると特殊信号発光機に点灯指示を出す.
- 列車にいる運転士は特殊信号発光機の発光を目で確認するとブレーキをかけて列車を緊急停車させる.

[4] システム安全性解析WG: “はじめてのSTAMP/STPA, 実践編”, 情報処理推進機構(2017)

STAMP WorkbenchでSTPA分析

STAMP Workbenchで導出されたアクシデント、ハザード、安全制約
(Loss、Hazard、Safety Constraints)

アクシデントID	アクシデント
A1	列車が"とりこ"状態の車と衝突する（通行者・列車の乗員が死傷）

ハザードID	ハザード
H1	"とりこ"発生時に特殊信号発光機が発光しない
H2	"とりこ"発生中に特殊信号発光機の発光が停止する
H3	特殊信号発光機の発光を運転手が視認できない

安全制約ID	安全制約
SC1	"とりこ"発生時に特殊信号発光機が発光すること
SC2	"とりこ"発生中は特殊信号発光機の発光が停止しない
SC3	特殊信号発光機の発光を運転手が視認できること

STAMP WorkbenchでSTPA分析

STAMP Workbenchで導出されたUCA表(Unsafe Control Action)

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	検知開始指示	踏切制御装置	障害物検知装置		(UCA1-N-1) 検知開始指示が出ていないので障害物が検知できない [SC1]	踏切が開いているのに特殊信号発光機が発光する	Too earlyで踏切が開いているのに特殊信号発光機が発光する (UCA1-T-1) Too lateで障害物検知が遅れ、特殊信号発光機の発光が遅れる [SC1]	-
2	発光指示	障害物検知装置	特殊信号発光機		(UCA2-N-1) 発光指示が与えられないので運転手が発光を視認できない [SC1]	"とりこ"非発生時に特殊信号発光機が点灯する	(UCA2-T-1) Too lateで発光指示が遅れ列車を停止できない [SC1]	-
3	消灯指示	障害物検知装置	特殊信号発光機		特殊信号発光機が点灯し続ける	(UCA3-P-1) "とりこ"発生中に特殊信号発光機が消灯する [SC2]	(UCA3-T-1) Too earlyで"とりこ"発生中に特殊信号発光機が消灯する [SC2] Too lateで"とりこ"解消後も特殊信号発光機が点灯し続ける	-
4	停止指示	特殊信号発光機	運転士		(UCA4-N-1) 特殊信号発光機が点灯せず列車を停止しない [SC1][SC3]	"とりこ"非発生時に特殊信号発光機が点灯する	(UCA4-T-1) Too lateで特殊信号発光機の発光が遅れ列車を停止できない [SC1]	-
5	ブレーキ作動指示	運転士	列車		(UCA5-N-1) 運転手が特殊信号発光機の発光を視認せず、列車が停止しない [SC3]	"とりこ"非発生時に列車を停止する	(UCA5-T-1) Too lateで列車停止が間に合わない	(UCA5-D-1) Too soonで列車停止が間に合わない
6	検知終了指示	踏切制御装置	障害物検知装置		踏切が開いているのに特殊信号発光機が発光する	(UCA6-P-1) "とりこ"発生時に検知終了指示が出ると特殊信号発光機が消灯する [SC2]	(UCA6-T-1) Too earlyで"とりこ"の発生を検知できず特殊信号発光等が発光しない [SC2] Too lateで踏切が開いているのに特殊信号発光機が発光する	-

モデル化

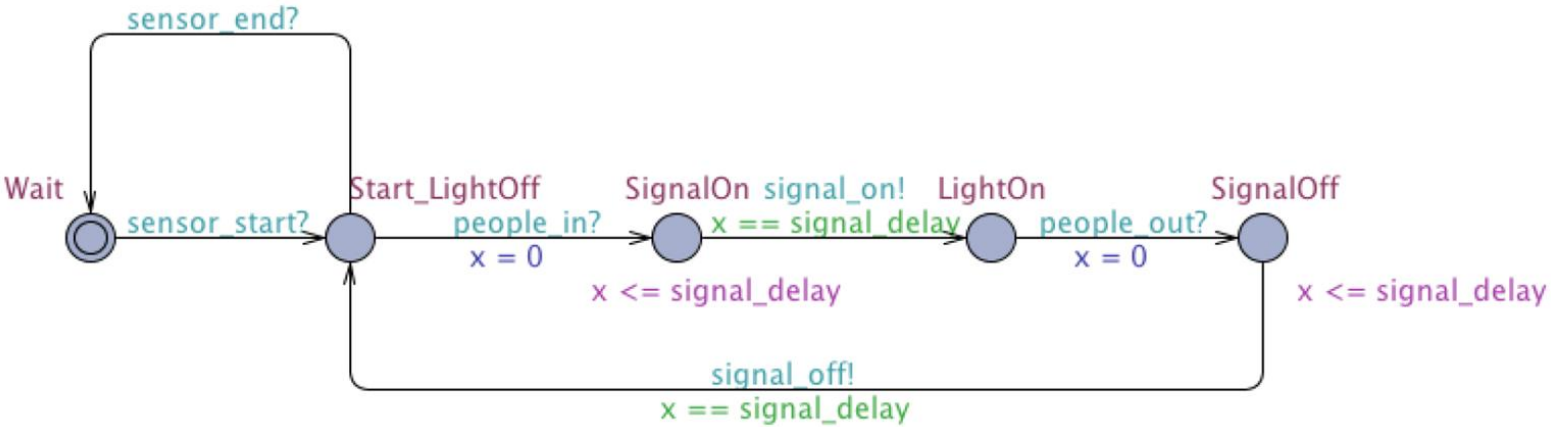
登場人物表 [5]

	登場人物	役割（安全関連責任）	備考
1	障害物検知装置	踏切遮断中に踏切内に車があるか否か検知し、車を検知すると特殊信号発光機に点灯指示を出す。 “とりこ”解消時に特殊信号発光機に消灯指示を出す。	
2	特殊信号発光機	障害物検知装置からの指示を受けて点灯・消灯する。	
3	通行車・人	踏切を通行する車。踏切遮断開始時に、踏切に進入してはならない。また踏切から退出しなければならない。 退出できずに滞留すると“とりこ”という。	
4	運転士	特殊信号発光機の発光を確認（視認）するとブレーキをかけて列車を緊急停止させる。（“とりこ”との衝突回避）	目視
5	列車	運転手に制御されて踏切に向かって進行中の列車	
6	踏切制御装置	列車の接近をセンサーで検知して踏切を遮断するとともに障害物検知装置に動作開始を指示する。また列車通過完了をセンサーで検知して踏切を開通するとともに障害物検知装置に動作終了を指示する。	
7	踏切遮断機	踏切制御装置から指示を受けて遮断・開通する	

[5] システム安全性解析WG: “はじめてのSTAMP/STPA, 実践編”, 情報処理推進機構(2017)

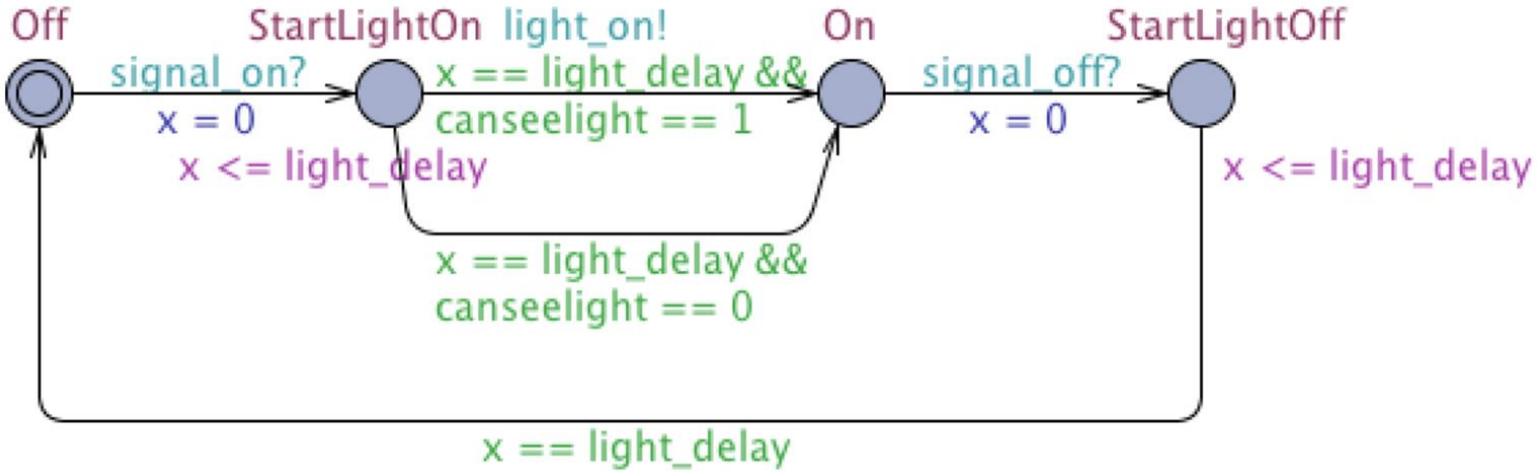
UPPAALのテンプレート
（時間オートマトンモデル）

障害物検知装置



- 警報開始センサーからのsensor_start信号を受け，検知を開始する
- 踏切内に通行車・人の滞留を検知したらsignal_on信号を送出し，通行車・人を検知しなければsignal_off信号を送出する
- 各信号の出力に時間遅れが発生することを考慮し，その長さをパラメータて指定できるようにした

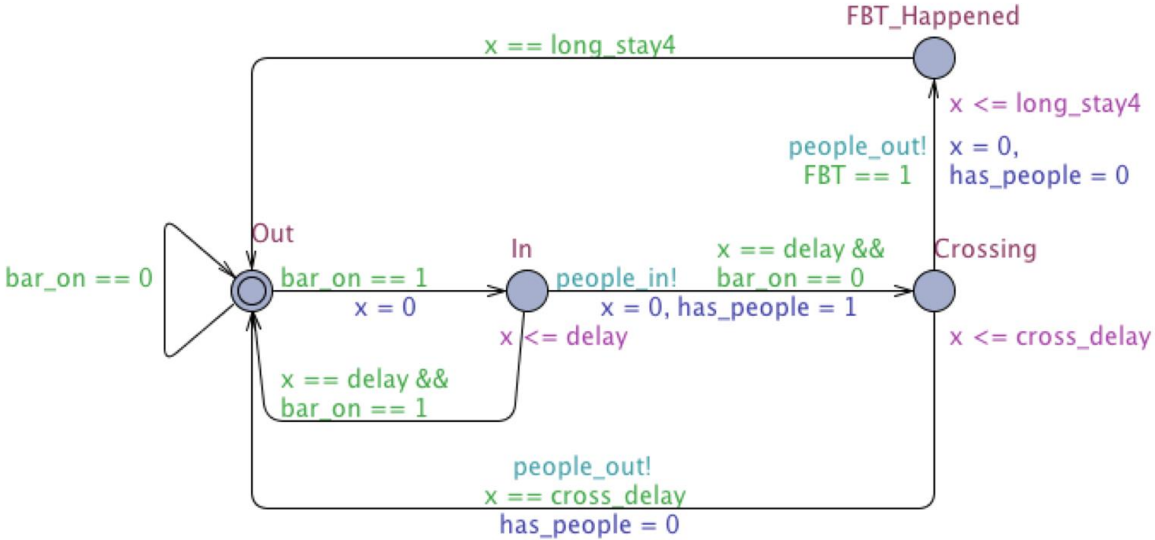
特殊信号発光機



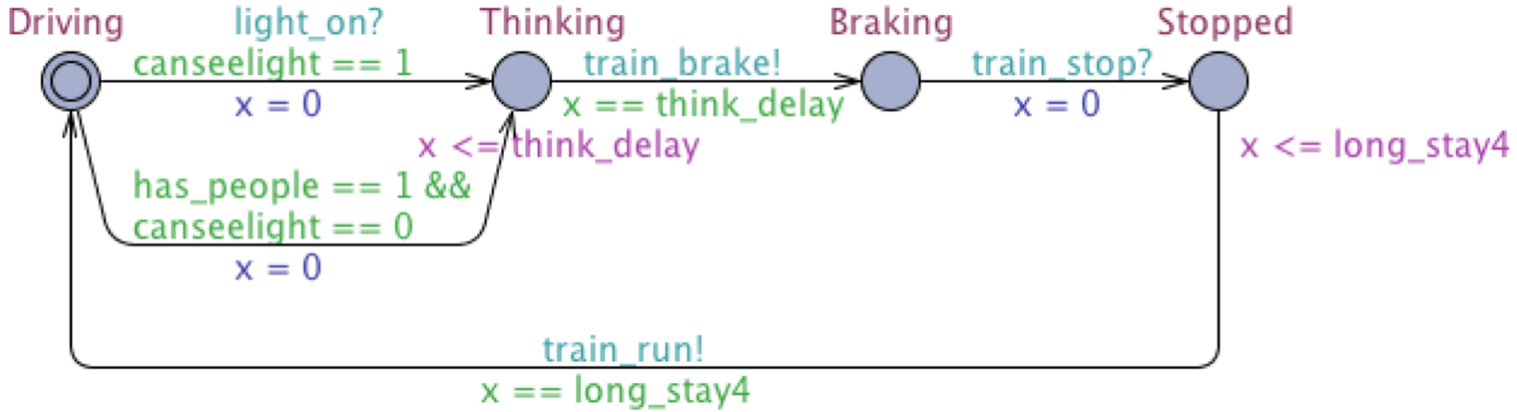
- 障害物検知装置によるsignal_on信号とsignal_off信号を受け，点灯・消灯する
- 運転士による特殊信号発光機の目視の可否を設定する
- canseelight変数を宣言し，見えるときにlight_on信号を送出し，見えなければ送出しない

通行車・人

- Inの状態で障害物検知装置によって検知していない場合はOut状態に戻る
- 検知している場合はCrossing状態になる
- モデルをループ可能にするため，FBT_Happened状態を追加し，一定時間後 (事故を処理する時間)，初期状態に戻るようにした

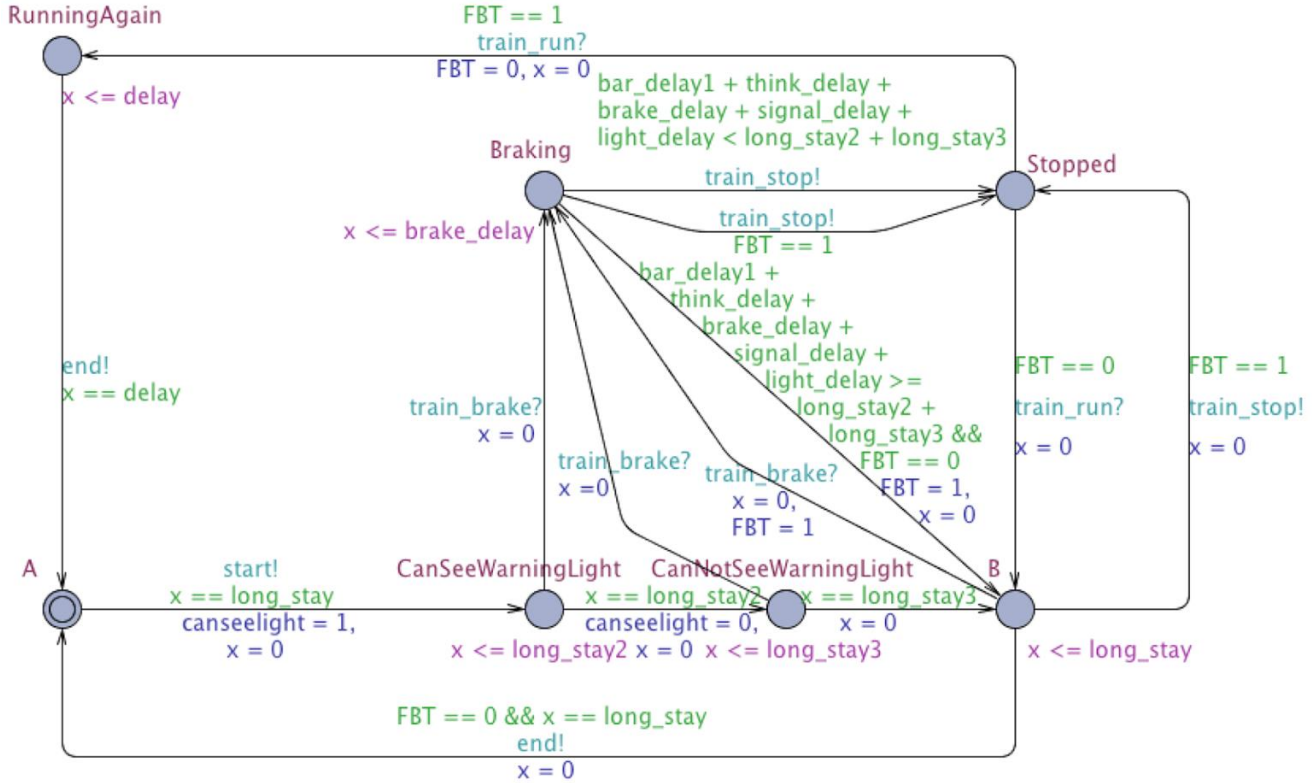


運転士

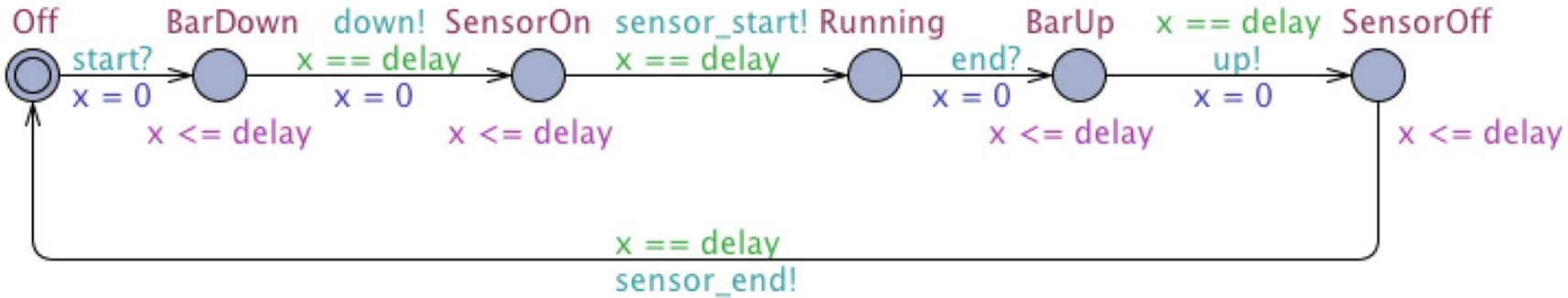


- 運転士は特殊信号発光機が見えるときに，特殊信号発光機からlight_on信号を受ける.
- 見えないときは，「とりこ」を目視で確認

列車

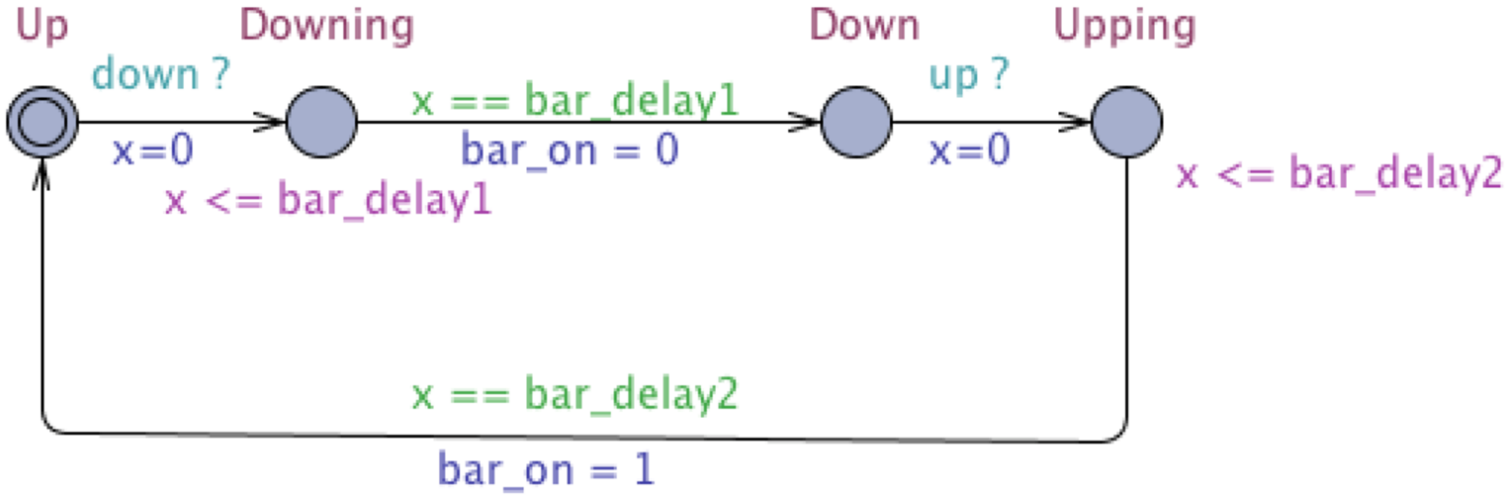

RunningAgain
FBT == 1
train_run?
FBT = 0, x = 0
x <= delay
bar_delay1 + think_delay +
brake_delay + signal_delay +
light_delay < long_stay2 + long_stay3
Braking
Stopped
train_stop!
x <= brake_delay
train_stop!
FBT == 1
bar_delay1 +
think_delay +
brake_delay +
signal_delay +
light_delay >=
long_stay2 +
long_stay3 &&
FBT == 0
FBT = 1,
x = 0
end!
x == delay
train_brake?
x = 0
train_brake?
x =0
train_brake?
x = 0,
FBT = 1
FBT == 0
train_run?
x = 0
FBT == 1
train_stop!
x = 0
A
start!
x == long_stay
canseelight = 1,
x = 0
CanSeeWarningLight
x <= long_stay2 x = 0
CanNotSeeWarningLight
x == long_stay2
canseelight = 0,
x <= long_stay3
x == long_stay3
x = 0
B
x <= long_stay
FBT == 0 && x == long_stay
end!
x = 0

踏切制御装置



- 警報開始センサーからstart信号を受けた遮断機が降下する (down) と，障害物検知装置に対し検知開始信号 (sensor_start) を送出する
- 警報停止センサーからend信号を受けて，遮断機を上昇させる (up) と，障害物検知装置に対し検知終了信号 (sensor_end) を送出する

踏切遮断機[6]



踏切遮断器は踏切制御装置からup信号，down信号を受けて，遮断機を上昇・降下させる

[6] 岡野浩三, 小形真平, 楊 盼, 岡本圭史: “STAMP/STPA 単線列車例題に対する時間オートマトンモデル検査の適用と考察”, 電子情報通信学会技術研究報告, 117 (477) pp.1-6 (2018)

試行結果

- 式(1)の成立を確認した

$$\mathbb{AG}(train.B \Rightarrow peopleandcar.Out) \qquad (1)$$

- この式は列車 (train) がB (踏切遮断機と警報停止センサー) にいるときには通行車・人 (peopleandcar) が踏切にいない (Out) ことを示す．すなわち，アクシデントにならないことを意味している．
- 次に，システムがdeadlockにならないように時間変数それぞれを変更し，式 (1) が成立しない状況を見つけた．具体的には以下の５つ状況がある．

(1) 運転士の反応時間	$(t \geq 13)$
(2) 列車のブレーキ時間	$(b \geq 28)$
(3) 踏切遮断機降下時間	$(b_1 \geq 21)$
(4) 特殊信号発光機発光時間	$(l \geq 7)$
(5) 障害物検知装置発行指示時間	$(s \geq 7)$

「長時間の操作」と「操作の遅れ」はパラメータを大きくすることで「操作せず」，「操作できない」にも対応できる．すなわち，ここで並べた状況は，モデルUCA表の「Not Providing」「Too early / Too late」と「Stop too soon / Applying too long」の各項目に対応できる．「Providing causes hazard」には別の工夫が必要である．

試行結果

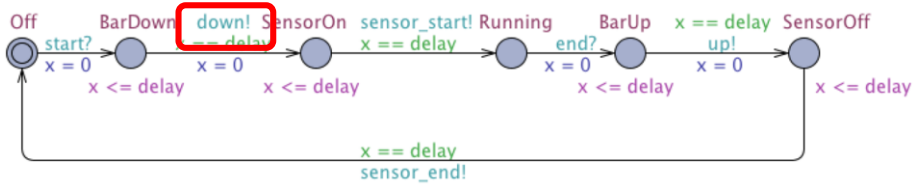
モデルの中にある時間に関する変数 (時間変数) の値を調整しながら，deadlock-freeにする.
得られた値：

時間変数		deadlock-freeになる値
(1) 運転士の反応時間	(t)	(1) $t = 5$
(2) 列車のブレーキ時間	(b)	(2) $b = 20$
(3) 踏切遮断機降下時間	(b_1)	(3) $b_l = 15$
(4) 特殊信号発光機発光時間	(l)	(4) $l = 1$
(5) 障害物検知装置発行指示時間	(s)	(5) $s = 1$
(6) Aから特殊信号発光機までの通信時間	(l_2)	(6) $l_2 = 25$
(7) 特殊信号発光機からBまでの通信時間	(l_3)	(7) $l_3 = 25$

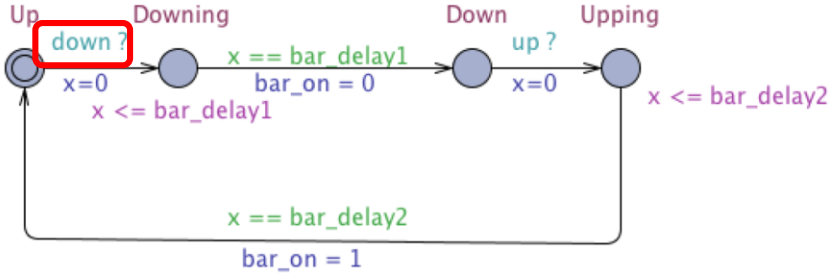
中間考察

以下の3つの問題の解決が必要

- モデル導出支援
- 時間変数の調整の自動化
  - ハザードシナリオを導出する際に，時間変数を一定範囲に設定し，ツールが自動的に探索し，希望値を満たす時間変数を自動導出する
- 構成要素の不具合に関するハザードシナリオの導出



踏切制御装置



踏切遮断機

連携に関する提案方法 (WIP)

- コントロールストラクチャ
  - イベント、アクションの抽出
- 登場人物
  - コンポーネントの同定

- STAMPWorkbenchの備考欄/役割欄の活用　→　時間オートマトンテンプレートの導出
  - 状態を明示、条件変数
  - テーブルを記述　or 自然語記述からの変換

分析手法

解析者は時間変数の制約条件を与える
ツールが入力パターンテンプレートの提示を支援する

線形計画法を用いて時間変数の範囲の上限、下限を決定する

(1) 運転士の反応時間 (t)
(2) 列車のブレーキ時間 (b)
(3) 踏切遮断機降下時間 (b_1)
(4) 特殊信号発光機発光時間 (l)
(5) 障害物検知装置発行指示時間 (s)
(6) Aから特殊信号発光機までの通信時間 (l_2)
(7) 特殊信号発光機からBまでの通信時間 (l_3)

$$\begin{cases} t+b+l+s \le l_2+l_3 \\ l=s=1<t<b_1<b<l_2=l_3 \end{cases}$$

$\Rightarrow$

$$\begin{cases} t+b+b_1+2<2l_2 \\ 1<t<b_1<b<l_2 \end{cases}$$

時間変数

New：変数の制約条件

最小値（or 最大値）の導出方法（線形計画法）

$$\begin{cases} l_2 = \frac{1}{2}k_1 + \frac{3}{2}k_2 + k_3 + \frac{1}{2}k_4 + 6 \\ t = k_2 + 2 \\ bl = k_2 + k_3 + 3 \\ b = k_2 + k_3 + k_4 + 4 \end{cases}$$

$$k_1' = 2k_1 \quad k_2' = 2k_2 \quad k_3' = 2k_3 \quad k_4' = 2k_4$$

$$\Rightarrow \begin{cases} l_2 = k_1 + 3k_2 + k_3 + k_4' + 6 \\ t = 2k_2' + k_3 + 3 \\ b_l = 2k_2' + k_3 + 3 \\ b = 2k_2' + k_3' + 2k_4' + 4 \end{cases}$$

$$\Rightarrow \begin{cases} l_2 = 6 \\ t = 2 \\ b_l = 3 \\ b = 4 \end{cases}$$

各時間変数の適切値(or 最大値)の探索

deadlockにならない範囲で、検査式を満たす各時間変数の最大値
deadlockにならない範囲で、安全制約を満たす値、満たさない値，etc
を探したい

各時間変数に対して、二分探索法を用いて探索

まとめ

- STAMP/STPA とモデル検査技術との連携の有用性を提示した
- STAMP Workbenchとモデル検査技術との具体的な連携方法について考察した

今後の課題

- 連携用プログラムの構築
- 研究室で開発中の時間オートマトンモデル検査ツールでSTAMP/STPA向けに反例導出や再現の機能を実現したい