UNISYS

STAMP/STPAにおける モデル検査の利用

2016年12月7日

日本ユニシス株式会社
総合技術研究所
青木　善貴

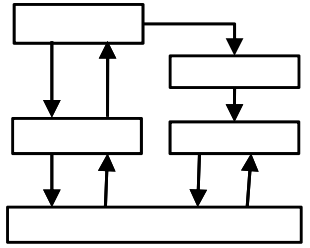
Foresight in sight

STAMP/STPAの手順概要

STPAによるハザード分析の手順

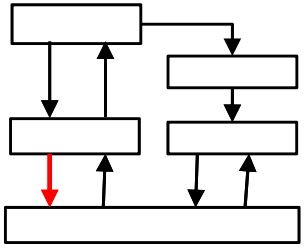
① Step0準備１：
事故、ハザード、安全制約の識別

② Step0準備２：
コントロールストラクチャの構築



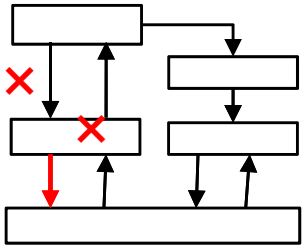
③ Step1：
UCA（Unsafe Control Action：安全ではないコントロールアクション）の識別

ガイドワード



④ Step2：
HCF（Hazard Causal factorハザード原因要因）の特定

ガイドワード



今回の提案（ This proposal ）

- Step2における HCF抽出をモデル検査を用いて支援する手法の提案

- コントロールアルゴリズムとプロセスモデルに注目してのハザード分析の支援

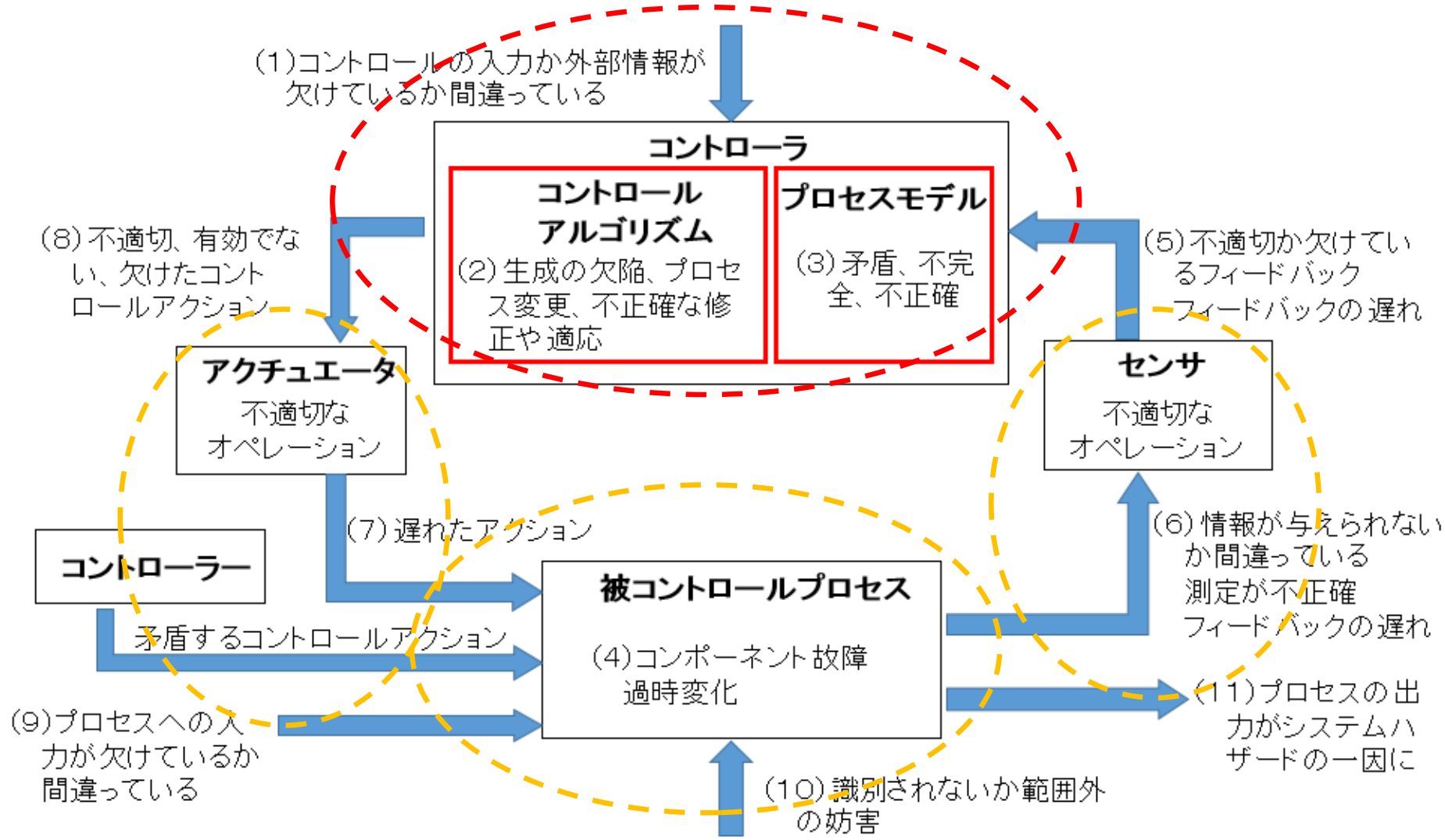
プロセスモデルは重要（Process model is important）

コントロールアルゴリズム(Control Algorithm)

＋　プロセスモデル(Process Model)

コントロールアクション(Control Action)

STEP 2　ガイドワード（Guide Word）



プロセスモデルの定義
(Process model definition)

- コントローラが認識すべき被コントロールプロセスの状態を定義しなければならない
- なおかつ、そこから矛盾を見つけなければならない

モデル検査の利用(Use of Model Checking)

- プロセスモデルを網羅的に検証する
  （Exhaustive verification of the process model)

プロセスモデルの状態を網羅的に検査するには、
モデル検査が有効と考える

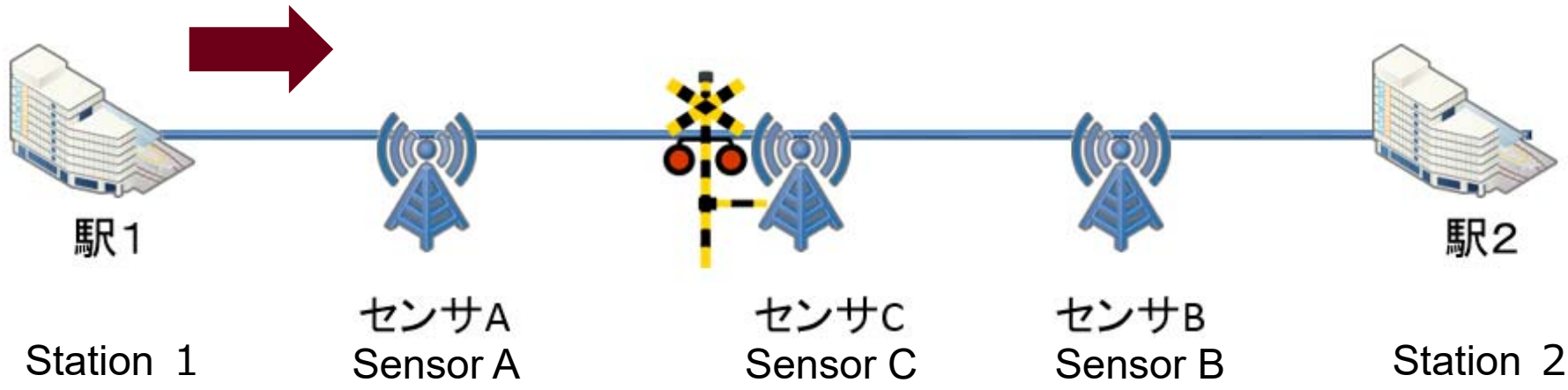
モデル検査を使うための課題（Problem）

- プロセスモデルのモデル化
  (Modeling of Process Model)

- コントロールアルゴリズムのモデル化
  (Modeling of Control Algorithm)

適用事例　概要（Case Study）

- IPAが公開している資料「はじめてのSTAMP/STPA～システム思考に基づく新しい安全性解析手法～」にある分析実施例「単線の駅中間踏切制御装置」
  - ◆ 警報開始センサA，Bは列車を検知すると踏切を鳴動させる.
  - ◆ 警報終止センサCは列車を検知すると踏切の鳴動を停止させる.
  - ◆ 警報終止センサCを通過した時点で，警報開始センサBをマスクする.
  - ◆ 警報開始センサBを通過した時点で，センサBのマスクを解除する.



アクシデント・ハザード・安全制約

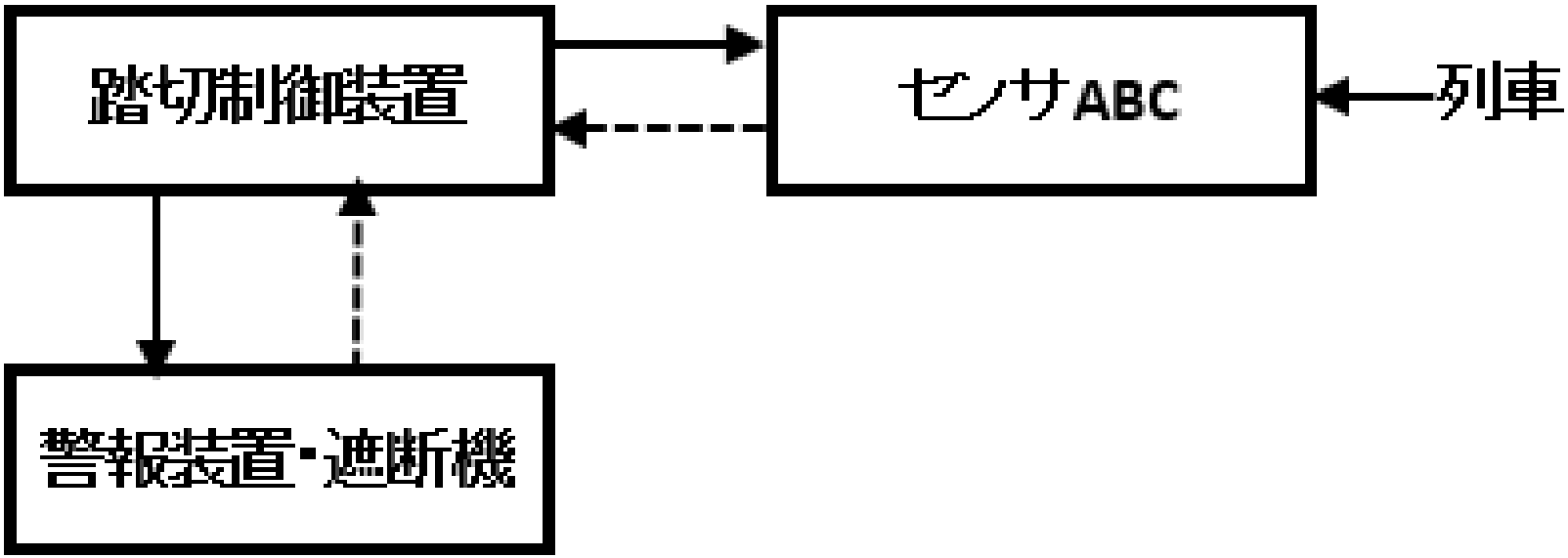
- アクシデント(Accident)
  - 列車と人もしくは車などが踏切内で衝突する
- ハザード(Hazard)
  - 列車が踏切通過中に警報が鳴動していない
- 安全制約(Safety Constraints)
  - 列車が踏切を通過中は、警報が常に鳴動している

コントロールストラクチャ(Control Structure)

- コントローラ(Controller)は「踏切制御装置」(railroad crossing controller)
- 被コントロールプロセス(Controlled Process)が「センサABC」と　「警報機、遮断機」(Alarm System)
- 「列車」(Train)はセンサに対する入力(Input)とする

コントロールストラクチャ(Control Structure)

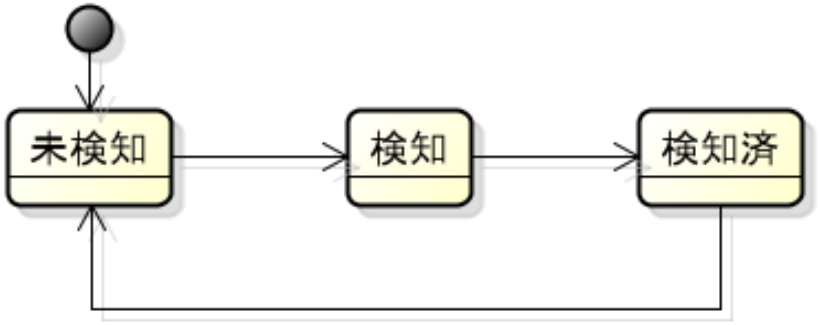
(Railroad Crossing Controller)　(Sensor A,B,C)　(Train)



(Alarm System)

プロセスモデルの状態(State of Process Model)

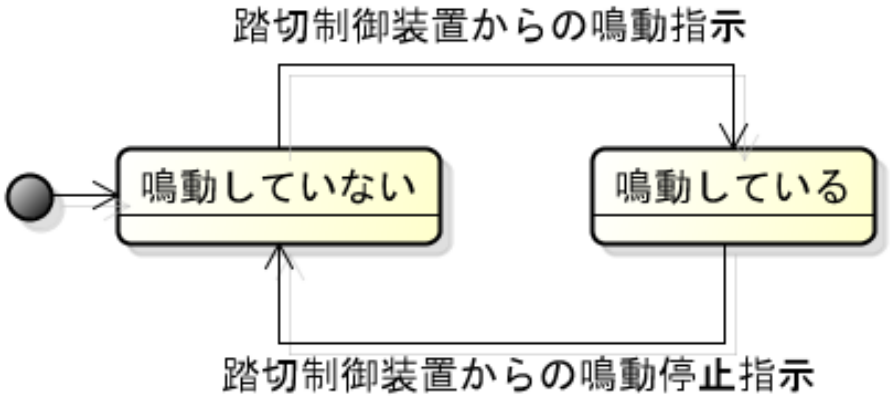
センサ信号A～B



コントローラからの視点

- センサについては信号の有無で見る
- 警報音鳴動装置については、鳴動の有無で見る

警報音鳴動装置



制約

進行方向 左⇒右

A通過回数>=C通過回数>=B通過回数

進行方向 右⇒左

B通過回数>=C通過回数>=A通過回数

コントロールアルゴリズム(Control Algorithm)

- センサA
  - 非検知⇒検知／非検知
  - 検知⇒検知／通過
  - 通過⇒非検知
- センサC
  - A通過回数＞C通過回数　かつ　非検知⇒検知／非検知
- 警報音鳴動装置
  - センサA検知⇒鳴動開始
  - センサC通過⇒鳴動停止

モデル検査の実施(Model Checking)

- モデル検査ツール　NuSMV

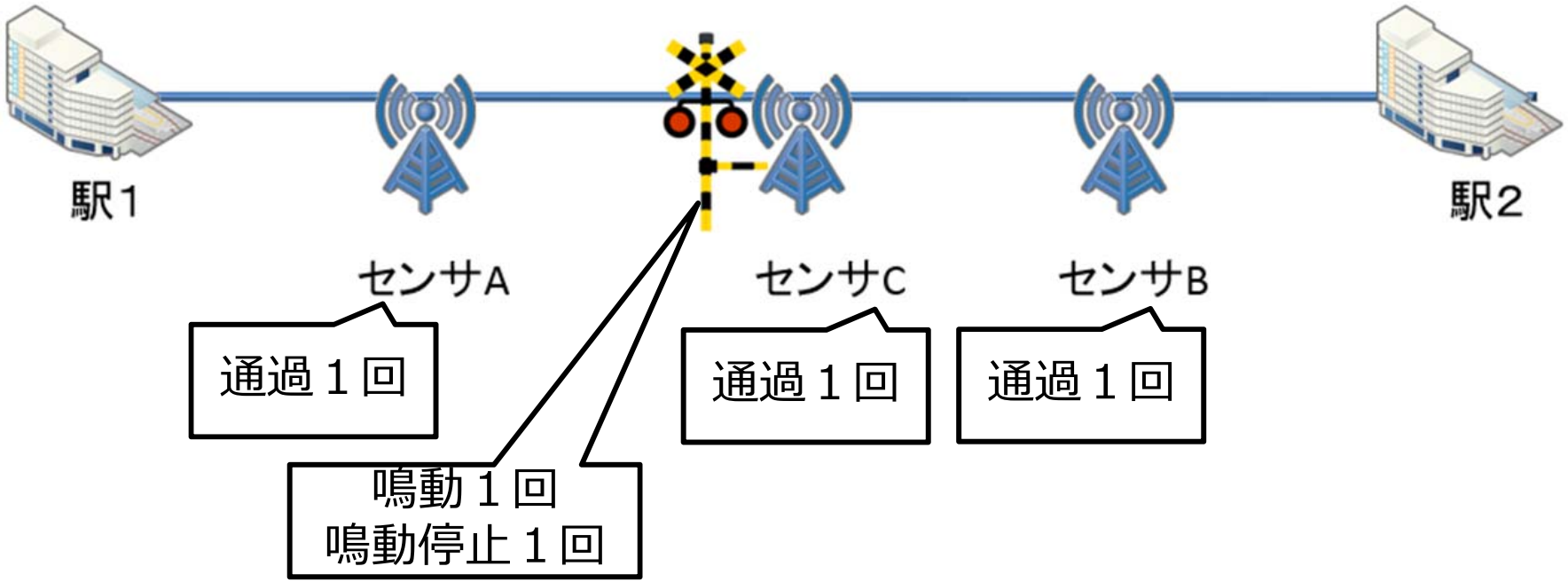
- 正常動作の検査(Inspection of normal operation)
  - デッドロックしない、各駅へ到達する、鳴動する、マスクする

- 安全制約の検査(Inspection of Safety Constraints)
  - 安全制約：列車が踏切通過中は警報が常に鳴動している
  - 検査式：列車が踏切通過中に警報が鳴動しないことは、決してない

検査式の検討

- 正常ならば、センサABCの通過回数、鳴動回数、鳴動停止回数は等しいはず

Number of Sensor A,B,C passage=Number of Alarm sounding
= Number of Alarm stopping



検証結果(Inspection Result)

検査式としては、

「 A通過回数＝B通過回数＝C通過回数　かつ

　警報鳴動回数＜A通過回数」となることはない

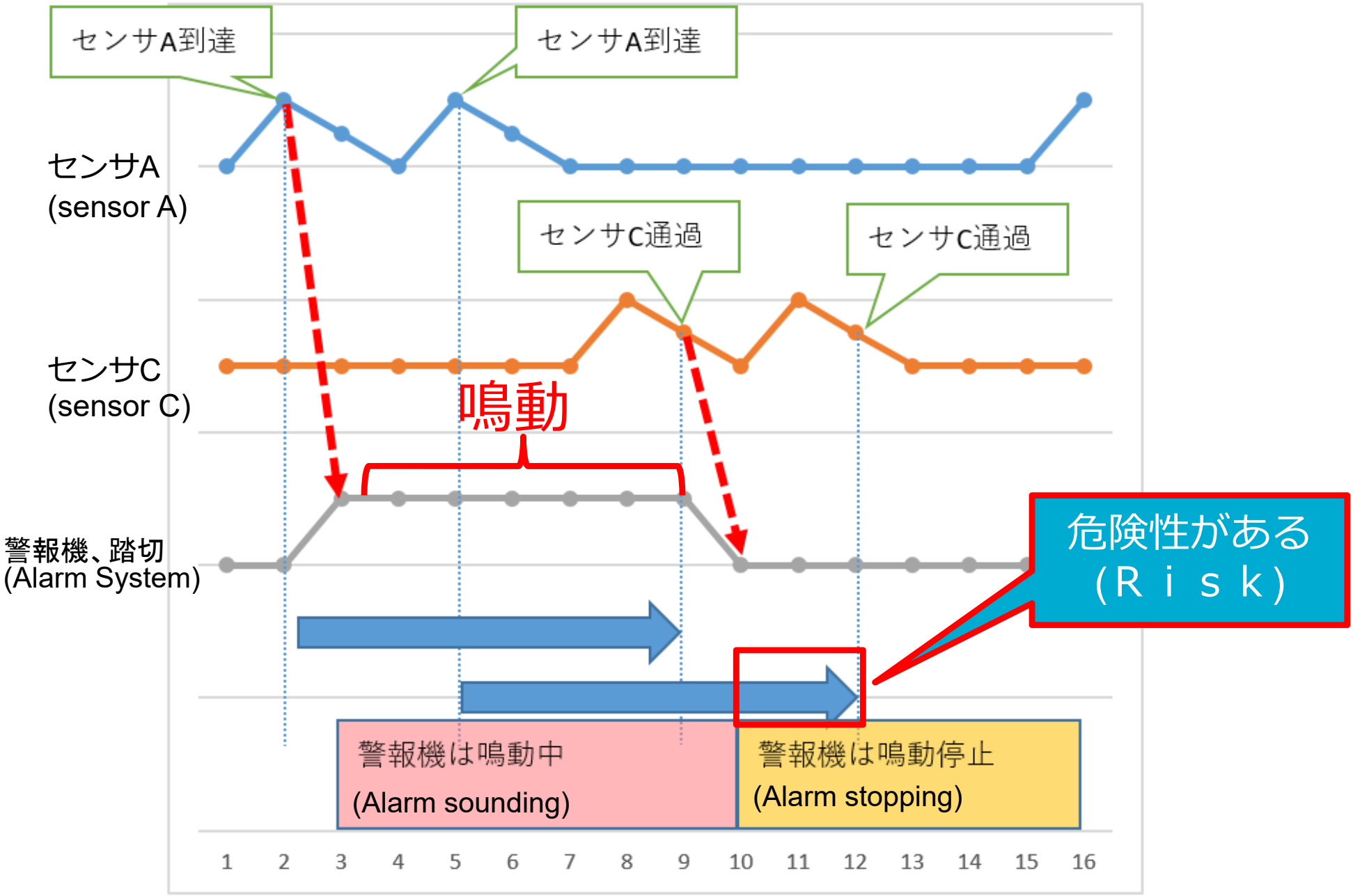
```
SPEC AG!((Sens.A_CNT=Sens.B_CNT &
                Sens.B_CNT=Sens.C_CNT) &
          (RUNG_CNT < Sens01.A_CNT))
```

検証結果は、「満たされない」(Not satisfied)

検証結果(Inspection Result)

- 反例を確認すると
  - A通過回数＝２回
  - B通過回数＝２回
  - C通過回数＝２回
  - 警報鳴動回数＝１回
  - 警報鳴動回数＝１回

反例解析(Counter Example)



考察

- 接近した状態で２台の列車が運行されると，後発の列車が踏切を通過中に，もう先発の列車が警報を解除する可能性がある

まとめ(Conclusion)

- HCF抽出において、モデル検査を利用することにより、網羅的な検証の支援ができることを示した

- プロセスモデルの状態から、安全制約の検査式が記述できない場合は、再度検討が必要

Foresight in sight

UNISYS