R-21

複数ロボットシミュレーションのSTAMP/STPAでの活用 ― STAMP/STPA本の題材を箱庭で実験してみた ―

久保秋 真（チェンジビジョン）, 森 崇（箱庭ラボ）, TOPPERS/箱庭WG

概要

複数システムが協働するシステムの安全を分析する手法としてSTAMP/STPA[1]がある. しかし, 分析で想定する状況実際に試すは難しく, 手法の適用や学習の妨げになっている. 「箱庭」は, 開発手法が異なる多様なシステムを混在してシミュレーションできるので, STAMP/STPA が想定する複数のシステムが相互動作する仮想環境の構築に向いており, うまく適用できれば, 安全分析分野での活用が期待できる. 本セッションでは, 事例にある踏切制御システム[2]を構築し, 安全分析シナリオのシミュレーションを紹介する.

対象システムの構成

対象システムである踏切制御システムの構成を図1に示す. 軌道は単線で双方向に列車が走行する. 踏切とその周辺には列車の通過を認識する「始動点, 終止点踏切制御子」がある.

近年の踏切は制御装置, 遮断桿（かん）, 警報灯, 警報笛で構成される. 踏切には他の安全対策機器も利用されているが, 事例の踏切には設置されていない.

図1. 踏切制御システムの構成

踏切制御システムの働き

1. 始動点踏切制御子A, Bが列車の侵入を検知すると, 踏切は警報音を鳴らし続け, 警報灯を点滅し続け, 遮断桿をおろす.
2. 終止点踏切制御子Cが列車が通過し終えたことを検知すると, 踏切は一定時間経過した後, 警報灯, 警報音を終止し, 遮断桿をあげる.
3. 列車がAから侵入した場合は, Cをマスク（センサーの入力を抑止）する.
4. 列車がBから侵入した場合は, Aをマスク（センサーの入力を抑止）する.

シミュレータの構成

シミュレーション環境には, 「箱庭」を用いる. 今回のシミュレーション環境の構成を図2に示す. 列車と踏切は各々独立しており, それぞれがUnity上の自分の仮想環境モデルと連携して動作する. ATCと異なり, 列車と踏切が直接やとりをせず, 各々の動作が仮想環境に及ぼす変化にしか依存していないことに注意.

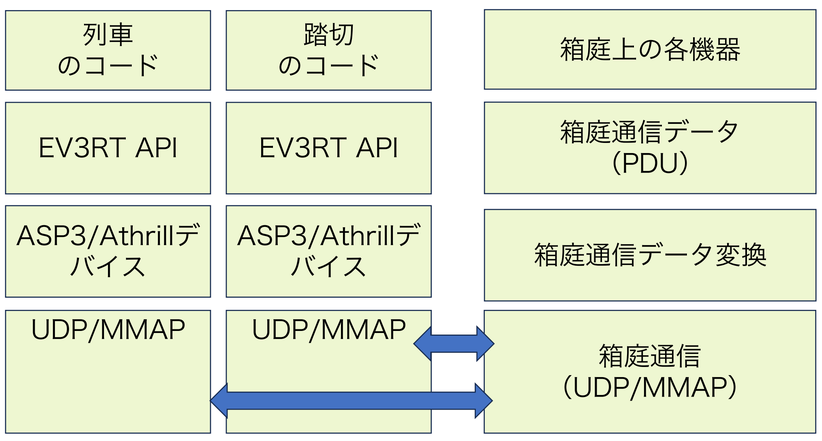

図2. シミュレーション環境の構成

STAMP/STPA事例の相互作用

STAMP/STPAでは, システムの構成要素間の相互作用に「危険の原因（ハザード）」が存在するとみて解析する. 事例の踏切における構成要素の相互作用を抽出して作成したコントロールストラクチャーを図3に示す.

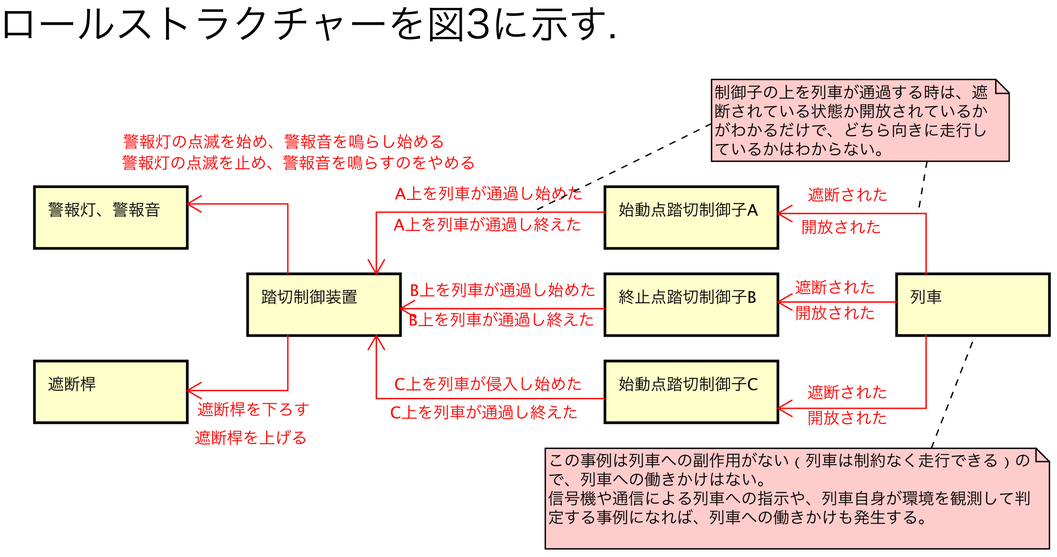

図3. 事例の踏切制御システムのコントロールストラクチャー

シミュレータによるシナリオの実施

シミュレータがあれば, 事例が想定する非安全なコントロールアクションに関わるシナリオを確認できる. 本セッションでは, 下記のようなシナリオについて, シミュレータで事象が確認できるデモンストレーションを実施し, 事例の記載に合致するか, 他に想定外のことが発見できるか試みる. シミュレータ実行中の様子を図4に示す.

シナリオ（1）

1. 始動点踏切制御子Aを列車が通過し, 制御装置は遮断桿を下ろす指示を出した.
2. 遮断桿が下りる前に列車が踏切を通過してしまった.

シナリオ（2）

1. 終止点踏切制御子Cに車両が停車してしまった.
2. そのまま時間が経過した場合や他の列車が近接した場合, 何が起きるか.

シナリオ（3）

1. 意図的に始動点踏切制御子Aや終止点踏切制御子Cのセンサーの故障を引き起こす.
2. このとき, 遮断桿を下ろすといった安全側に倒す動作ができるか.

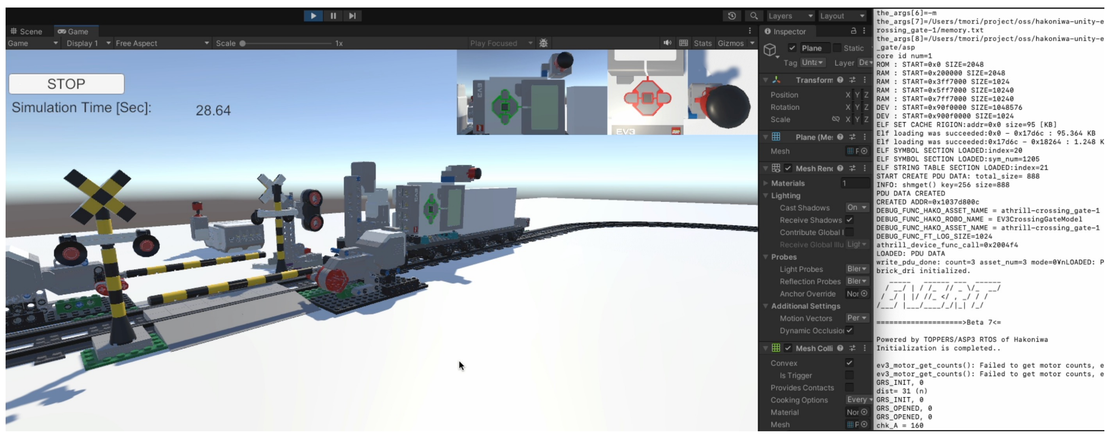

図4. 箱庭を使ってシミュレーションを実施している様子

おわりに

箱庭によって, STAMP/STPAの分析事例をシミュレーション環境で動かせるようになった. 箱庭が, 安全分析そのものの支援に活用できるよう, 検討を進めたい.

[1] Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
[2] IPA, はじめてのSTAMP/STPA（実践編）2章, IPAsソフトウェア高信頼化センター, 2017.