統計的モデル検査法を用いたSTAMP/STPAにおけるシナリオのリスク分析

辻 光顕[1,a)]　高井 利憲[1]　柿本 和希[1]　石濱 直樹[2]　片平 真史[2]　飯田 元[1]

概要：近年，ソフトウェアを中心としたシステムに対する新たな安全分析手法として STAMP/STPA が注目されている．STAMP/STPA では，システムに対する安全コントロールストラクチャを作成し，そこからハザードに至るシナリオおよび安全対策を導出する．一方で，効率的にシステムの安全性を高めるためには，リスクに基づくシナリオの優先付けによる安全対策の検討が必要であると考えられる．そこで本稿では，統計的モデル検査法を利用してシナリオに対するリスクを評価する手法について述べる．特に，踏切制御システムを題材として，安全コントロールストラクチャやシナリオなどを系統的に形式化する方法について説明する．

Risk Analysis of Scenarios based on STAMP/STPA Using Statistical Model Checking

1. はじめに

近年，システムの基幹的役割をソフトウェアが担うようになったことで，システムの故障によらないハザードに対する安全分析の重要性が増している．こうしたハザードを分析するための新たな手法として STAMP/STPA[2] が注目されている．STAMP/STPA では，まず対象システムにおける機能間の相互作用を安全コントロールストラクチャとして記述する．次に，その機能間における認識の齟齬を識別しハザードに至るシナリオを作成する．そして，各シナリオに対する安全対策を検討する．

一方で，開発期間やコストが限られた状況下では，識別されたシナリオに対する安全対策の効果的な反映が重要となる．そのためには，各シナリオにおけるリスク値 (発生確率と危険度の積) の評価による優先付けが有効であると考えられる．

リスク評価の考え方が用いられている対象として，例えば鉄道分野では RAMS と呼ばれる国際規格 (IEC 62278) が挙げられる．RAMS 規格では，システムに対するリスクベースによる安全分析および設計手法の必要性が述べられている．また，自動運転分野では，ドイツの自動運転戦略 (Pegasus Project)[1] がシナリオベースによるリスク分析を提案しており，リスクの高いものから優先的にテストを行うための手法が研究されている．

そこで本研究では，STAMP/STPA におけるシナリオの定量的なリスク評価を統計的モデル検査法によって行う手法について提案する．特に，シナリオを形式的なモデルで表現するために，STAMP/STPA におけるモデルを系統的に形式化する方法について述べる．

2. 提案手法

ここでは，今回の例題として用いる踏切制御システムの概要やシナリオ，リスク評価結果について述べる．

2.1 踏切制御システムの概要

ここでは，北村の報告 [3] を参考に，例題として用いる踏切制御システムおよび，そのシナリオについて述べる．図 1 に想定するシステムの構成を示す．また，図 2 に今回対象とするシステムの安全コントロールストラクチャを示す．ここでは，センサーやアクチュエータ等を含めたモデルを対象とする．連動制御装置は在線情報を基に信号を制御して列車の進路を決定する．また，踏切制御装置は列車の接近に応じて遮断器を制御するものとなっている．

[1] 奈良先端科学技術大学院大学
Nara Institute of Science and Technology (NAIST)
[2] 宇宙航空研究開発機構
Japan Aerospace Exploration Agency (JAXA)
[a)] tsuji.mitsuaki.tg5@is.naist.jp

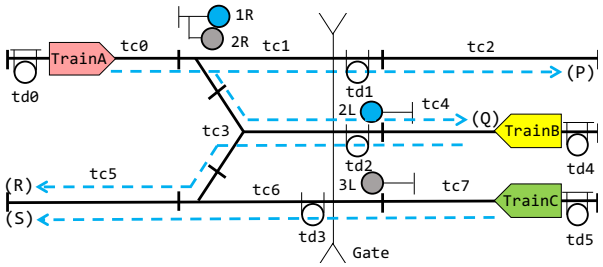

図 1　想定する踏切制御システムの構成

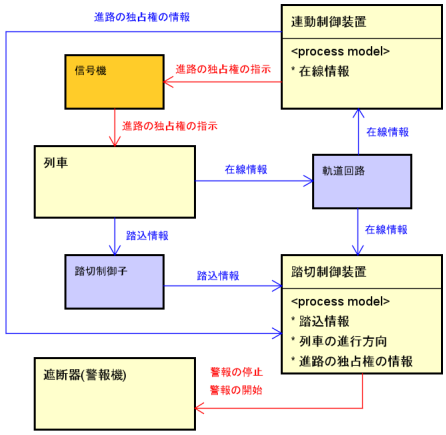

図 2　対象システムの安全コントロールストラクチャ

2.2　シナリオの例

2.1 節におけるシステムのもとで，ここでは 3 つのシナリオの例を考える．この例では，列車が TrainA，TrainB，TrainC の 3 台ある．また，tc0 から tc7 は在線検知に用いる軌道回路，td0，td4，td5 は列車接近検知を行う始動点であり，td1，td2，td3 は警報を停止するための終動点を表す．1R，2R，2L，3L は進路の独占権を表す信号であり，図中の矢印で示された P，Q，R，S の進路にそれぞれ対応する．また，中央の縦棒記号は踏切を示している．以下に，各シナリオの例に関する概要を示す．

(HS1)　信号 (1R,2R,2L,3L)=(青, 赤, 青, 赤) とする．TrainA が始動点 td0 に進入し警報開始する．その後，TrainB が tc3 に進入するが，踏切制御装置が 1R と 2R の進路を区別しなかったために，踏切制御装置が 15 秒以内に TrainA が tc3 に進入したと誤判断．異常検知を行い警報の鳴動が継続する．

(HS2)　信号 (1R,2R,2L,3L)=(赤, 青, 赤, 青) とする．TrainA が始動点 td0 を通過後に tc3 に進入するが，その後に TrainC が tc6 に進入したことで，踏切制御装置は TrainA がバックして tc3 から tc6 に進行したと誤判断．踏切に接近する列車がいないと判断して警報の鳴動が停止し，無遮断状態で列車が踏切を通過する．

(HS3)　信号 (1R,2R,2L,3L)=(赤, 青, 赤, 青) とする．TrainC が始動点 td5 に進入し警報開始した直後，後続の列車 (TrainC2 とする) が tc7 に進入する．TrainC が終動点 td3 に進入することで接近する列車がいないと誤判断し，TrainC2 が無遮断状態の踏切を通過する．

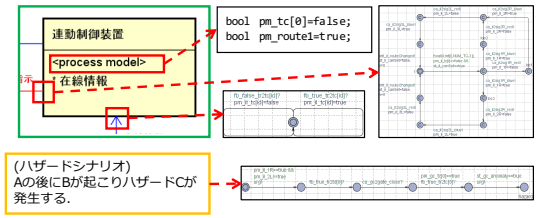

図 3　モデルの形式化イメージ

表 1　リスク分析結果

シナリオ	発生確率	影響度	リスク値
HS1	[0.00487, 0.00687]	2	[0.00974, 0.01374]
HS2	[0.00597, 0.00797]	3	[0.01791, 0.02391]
HS3	[0, 0.00199]	3	[0, 0.00597]

2.3　モデルの形式化

各シナリオの発生確率を求めるために，図 2 およびシナリオを Uppaal SMC によって形式化する．そのイメージを図 3 に示す．ここでは，STAMP/STPA のハンドブック [2] で述べられている損失に繋がるシナリオの分類に従って変換方法を検討した．形式モデル上でシナリオを表現するため，コンポーネントの入出力およびプロセスモデル，コントロールアルゴリズム，センサやアクチュエータなどを Uppaal SMC 上のオートマトンで表現する．ただし，形式化する機能の振る舞いは，簡単化のためハザードに関連すると考えられるものに限定している．また，シナリオを観測するためのオートマトンについても定義する．

2.4　統計的モデル検査法によるリスク分析

各シナリオの検証結果を表 1 に示す．定性的なモデル検査によって反例を分析したところ，シナリオがモデル上で再現できることが確認できた．ここでは，リスクの影響度や，モデルに含める列車の運行頻度などの数値を仮定している．統計的モデル検査法によって得られた確率値は 95% 信頼区間として得られている．シナリオ 3 については，実際には起こり得ないものであり，こうしたハザードについても定性的なモデル検査を行うことで発生の有無を検証できた．

謝辞　本研究を進めるにあたり，ご助言，ご協力頂きました仙台高専の岡本圭史准教授，JR 東日本の北村知様に感謝申し上げます．

参考文献

[1]　https://www.pegasusprojekt.de/en/home
[2]　N. G. Leveson and J. P. Thomas. STPA Handbook. 2018.
[3]　北村知. JR 東日本における STAMP 活用の取り組み. *SEC journal*, vol.13, no.4, pp.30–37, 2018.