2A-06

異常な状態遷移の生成により STAMP/STPA に基づくハザード要因を抽出するアルゴリズムの検討

笹　晋也†　　太田原　千秋†

株式会社日立製作所†

1. はじめに

システムのセーフティ・セキュリティを確保する上で，発生し得るハザードとその要因を設計段階から特定することが重要である．設計レベルで利用可能なハザード分析手法の 1 つが STAMP/STPA [1] であり，コントローラー，プロセス，コントロールアクション（CA），フィードバック（FB）からなる制御ループ（図 1）の組み合わせとしてシステムを捉える．そして，CA が与えられない，与えられる，早すぎる/遅すぎる/順序が誤っている，停止が早すぎる/適用が長すぎるという不安全な CA（UCA）がハザードの要因になるという考えに基づき，UCA を抽出することでハザードの要因を分析する．本稿では，UCA 抽出プロセスを自動化する手法を検討する．

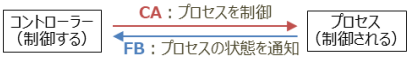

図 1　制御ループ

2. 課題

STAMP/STPA の分析対象システムが複雑，または分析者の経験や知見が不足している場合，UCA の見落としが多くなるという課題がある．時間オートマトンを用いた STAMP/STPA の自動化が提案されている[2] が，時間パラメータの変化のみでは CA が与えられる，順序が誤っているという UCA を探索しきれないという課題がある．

3. 提案手法

課題の解決に向け，CA が与えられない，与えられる，早すぎる/遅すぎる/順序が誤っているという UCA を機械的に抽出する手法を検討した．提案手法では CA の欠落・予定外の発動という事象を組み合わせることで UCA の抽出を可能にした．

本稿では，図 2 の踏切システム[3] を分析対象とする．このシステムは列車，センサ A～C，制御装置，踏切からなり，列車が駅 A から駅 B まで移動する場合の動作は以下の通りである．

- センサ A が通過開始を検知，制御装置に通知
- 制御装置は踏切遮断指示を出す
- センサ C が通過終了を検知，制御装置に通知
- 制御装置は踏切解放指示を出し，センサ B をマスク
- センサ B が通過開始を検知，制御装置に通知
- 制御装置はセンサ B をマスクしているため，踏切遮断指示を出さない
- センサ B が通過終了を検知，制御装置に通知
- 制御装置はセンサ B のマスクを解除

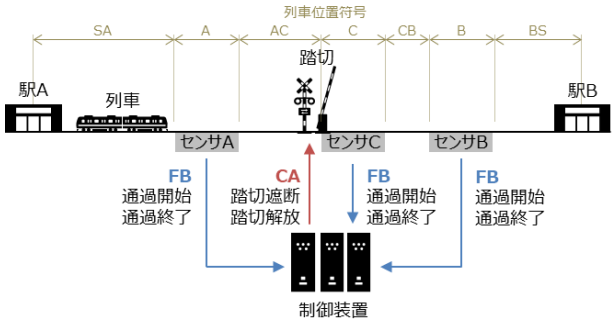

図 2　踏切システム

文献[3] ではマスクを踏切への CA としているが，踏切遮断指示の発出判断には制御装置がマスク状態を把握する必要があるため，本稿では制御装置内部でブーリアンのパラメータ mask_a, mask_b を変更する処理とする．また，次にマスクするセンサを表すパラメータ next_mask を持っているものとする．更に，以下では CA と FB をシグナルと総称する．

提案手法の入力情報を図 3 に示す．シグナルは FB と CA を区別する Type，発動タイミングを指定する Condition，引き起こすパラメータ変化を指定する Transition をプロパティとして持つ．Condition において，Issued[シグナル]はシグナルが発動したタイミングを，Become[条件]は条件が満たされるようになったタイミングを表す．Transition は（事前条件）⇒（変化後のパラメータ）の形式で表現されており，例えば踏切遮断指示である close シグナルは直前の状態によらず crossing パラメータを CLOSE に設定する．自発変化はシステム外部の要因によるパラメータ変化を指し，Condition が発生するための必要条件，Transition が発生するパラメータ変化を表す．ハザードとしては，ハザードが発生したと判断するパラメータの条件を入力する．初期

Research on an algorithm to derive STAMP/STPA-based hazard factors by generating erroneous state transitions
† Shinya Sasa, Chiaki Otahara・Hitachi, Ltd

条件は初期状態でのパラメータの値を指定する．

シグナル（一部のみ記載）

Name	Type	Condition	Transition
close	CA	(Issued[sensor_a_on] AND mask_a=FALSE) OR (Issued[sensor_b_on] AND mask_b=FALSE)	NONE ⇒ crossing=CLOSE
sensor_a_on	FB	Become[train=a]	—
sensor_a_off	FB	Become[train!=a]	NONE ⇒ next_mask=B AND mask_a=FALSE

自発変化

Name	Condition	Transition
train_right	train!=BS	train=SA ⇒ train=A train=A ⇒ train=AC train=AC ⇒ train=C train=C ⇒ train=CB train=CB ⇒ train=B train=B ⇒ train=BS
train_left	train!=SA	train=BS ⇒ train=B train=B ⇒ train=CB train=CB ⇒ train=C train=C ⇒ train=AC train=AC ⇒ train=A train=A ⇒ train=SA

ハザード

ID	Condition
H1	train=C AND crossing=OPEN

初期条件

Parmeter	Value
train	SA
crossing	OPEN
mask_a	FALSE
mask_b	FALSE
next_mask	B

図 3　入力情報

図 4 は提案手法で生成されるパターンデータであり，これにより UCA が表現される．状態遷移はパラメータの時間変化を表し，予定シグナルリストは発動条件が満たされたシグナルのリストである．イベント履歴はシグナル・自発変化の発生履歴であり，Time=t のイベントにより状態 No.t から No.(t+1)へ遷移する．Status は，Normal が仕様通り発生したこと，Provided が予定外のシグナルが発生したこと，Not provided が予定されたシグナルが発生しなかったことを表す．

状態遷移

No.	State
0	train=SA, crossing=OPEN, mask_a=FALSE, mask_b=FALSE, next_mask=B
1	train=A, crossing=OPEN, mask_a=FALSE, mask_b=FALSE, next_mask=B
2	train=A, crossing=OPEN, mask_a=FALSE, mask_b=FALSE, next_mask=B
3	train=A, crossing=CLOSE, mask_a=FALSE, mask_b=FALSE, next_mask=B
4	train=AC, crossing=CLOSE, mask_a=FALSE, mask_b=FALSE, next_mask=B
5	train=AC, crossing=CLOSE, mask_a=FALSE, mask_b=FALSE, next_mask=B
6	train=AC, crossing=OPEN, mask_a=FALSE, mask_b=FALSE, next_mask=B
7	train=C, crossing=OPEN, mask_a=FALSE, mask_b=FALSE, next_mask=B

イベント履歴

Time	Event	Status
0	train_right	Normal
1	sensor_a_on	Normal
2	close	Normal
3	train_right	Normal
4	sensor_a_off	Normal
5	open	Provided
6	train_right	Normal

予定シグナルリスト

Name
sensor_c_on

図 4　パターンデータ

提案手法のアルゴリズムを図 5 に示す．探索制限は，イベント履歴が一定数以下である，Status が Provided または Not provided である発生イベントがそれぞれ 1 個以下かつ同じイベントである，という 2 条件とする．この条件のもとで，予定シグナルが正しく発動(A)，予定シグナルが発動しない(B)，自発変化が発生(C)，予定にないシグナルが発動(D)という事象を組み合わせてパターンを生成し，ハザードに至るものを出力する．イベント履歴における Status が Provided, Not Provided であるイベントの存在/非存在，それらの Time の前後関係により，CA が与えられない，与えられる，早すぎる/遅すぎる/順序が誤っているという UCA が表現される．

4.　評価

踏切システムに提案手法を適用した結果，イベント履歴数の上限を 7 に設定すると，踏切通過後に踏切遮断指示が遅れて与えられる，踏切遮断指示が与えられない，踏切通過前に踏切解放指示が与えられるという UCA に該当する 6 パターンが出力され，本手法のスコープで文献[3]の分析結果と一致することが確認できた．これにより，分析者の経験・知見によらず UCA が抽出されることを確認した．

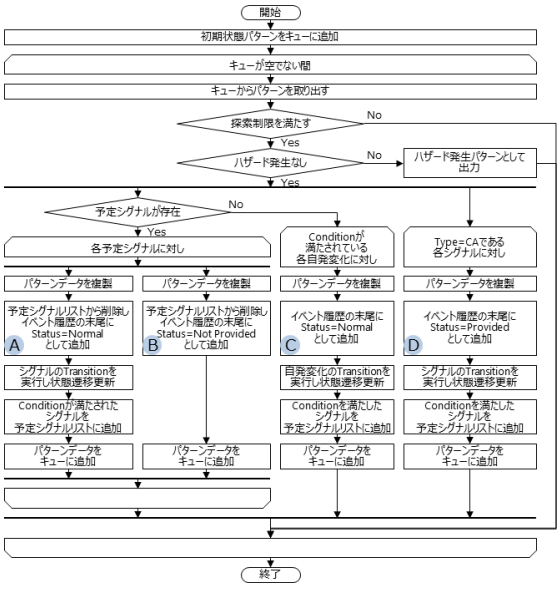

図 5　UCA 抽出アルゴリズム

5.　今後の課題

提案手法は瞬間的な CA のみ考慮しており，停止が早すぎる/適用が長すぎるという UCA をカバーしていない．より広いシステム・UCA をカバーできるよう手法の拡張を検討する．また，イベント履歴数の上限が小さいと UCA が不十分となる一方，大きいと組み合わせ爆発が起きるため，適切な値を決定する手法も検討予定である．

参考文献

[1] N. G. Leveson: Engineering a Safer world: Systems Thinking Applied to Safety, MIT press, 2011.
[2] P. Yang, R. Karashima, K. Okano, and S. Ogata: Automated inspection method for an STAMP/STPA – Fallen Barrier Trap at Railroad Crossing –, Procedia Computer Science, Vol.159, pp.1165-1174, 2019.
[3] 独立行政法人情報処理推進機構：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～，https://www.ipa.go.jp/files/000051829.pdf, 2016. [2021/12/15 参照]