システム理論に基づく安全性解析手法に関する調査研究

日本大学　理工学部　応用情報工学科　准教授　高橋　　聖

１．はじめに

鉄道システム，特に列車制御システムには高い安全性が求められている。列車制御システムにはコンピュータが用いられており，高機能化に伴いますます大規模かつ複雑化している。そして，システム同士のみならず，人とシステムの間の複合的な原因による障害も懸念される。

鉄道システムの安全性を確保するための国際規格として，IEC 62278（RAMS 規格）がある [(1)]。IEC 62278 では，安全性解析手法として，従来から広く用いられている FTA（Fault Tree Analysis）や FMEA（Failure Mode and Effect Analysis）を推奨している。これらの手法はハードウェアに関する解析には適しているが，ソフトウェアも含めたシステムの解析には限界がある。

このような中，近年コンピュータを含んだ複雑なシステムの安全性解析手法として，システム理論に基づく事故の発生過程のモデルである STAMP（Systems-Theoretic Accident Modeling and Processes）が，マサチューセッツ工科大学の Nancy G. Leveson により提唱されている [(2)]。STAMP は，ソフトウェアも含めたシステムの機能部分に着目し，複数のコントローラが介在する複雑なシステムの安全性解析が可能である。また，システムを構成するコンポーネントに不具合がなくても，それらの組み合わせによる不具合についても解析できる手法である。

本調査研究では，この STAMP に代表されるシステム理論に基づく安全性解析手法とその適用事例について調査し，将来的に STAMP を鉄道システムに適用する際の知見を得ることを目的とする。

２．システム理論に基づく安全性解析手法：STAMP

STAMP は安全が守られるために必要なルールである「安全制約（safety constraints）」を守るために，制御アクションを明確にした「コントロール構造（safety control structure）」を構築することに特徴がある。そして，ヒューマン要素も含んだ対象アイテムのコントロール構造を構築することで，アイテム（機能を実装するシステムまたはシステム群）が複雑であっても，ハザードにつながる不適切な制御アクションの潜在原因の識別が，従来の安全性分析手法に比べ，短時間かつ高い網羅性で行えるとして近年注目されている。

STAMP は安全性解析のモデルであり，次の 3 つのツールによって運用する。すなわち，(1) ハザード分析のためのツールである「STPA（System Theoretic Process Analysis）」, (2) 事故分析のためのツールである「CAST（Causal Analysis）」，そして (3) セキュリティに特化したハザード分析のためのツールである「STPA-sec」である。この中で, 高安全なシステム開発を進める上で, STPA が特に有用である。

STPA は以下に示すような 2 段階の準備と，2 つの STEP により実施する。

準備 1：ハザードおよび安全制約の識別
準備 2：コントロール構造の構築
STEP 1：不適切な制御アクションの識別
STEP 2：潜在原因の識別

準備 1 のハザードおよび安全制約の識別では，人への被害など，対象システムに想定される，アクシデントを引き起こす恐れのあるハザードを列挙していく。そして，それぞれのハザードに対する安全制約を識別する。

準備 2 のコントロール構造の構築では，まずアイテムを構成する機能部分を抽出する。機能部分として，制御対象，コントローラ，アクチュエータ，センサ等がある。コントローラからの制御命令がアクチュエータに出力され，制御対象を動作させる。制御対象の状態をセンサが捉え，コントローラにフィードバックする。コントロール構造は，このような制御ループによって表現される。コントロール構造を構築することで，各機能部分の入出力関係が明確になる。ここで構築したコントロール構造にもとづき，STEP 2 の「潜在原因の識別」が実施される。

STEP 1 の不適切な制御アクションの識別では，対象とするアイテムの持つ制御アクションについて，以下に示すような制御アクションに関する 4 つの不適切な状態をガイドとして，不適切な制御アクションを識別する。

(1) 安全のための制御アクションが設置されていない
(2) ハザードにつながる安全ではない制御アクションが設置されている
(3) 制御アクションのタイミングが遅すぎる，早すぎる，または定められた順序に設置されていない
(4) 制御アクションが設置されているが，すぐに止まる，もしくは適用が長すぎる

STEP 2 の潜在原因の識別では，STEP 1 で識別された不適切な制御アクションをもとに，これらのアクションが生じる原因を，準備 2 で構築したコントロール構造に沿って検討する。

3．STAMP の適用事例

STAMP のツールの 1 つである STPA の適用事例としては，高エネルギー源に対する安全扉によるインターロックの例や [(2)]，電車の自動扉制御の例がある [(3)]。これらの例の詳細は文献に譲り，ここでは，コンポーネントの機能不全が重大なアクシデントにつながる恐れがある対象アイテムとして，二輪車の電子制御スロットルについて STPA を実施した例を説明する。

表 1 に準備 1 のハザードおよび安全制約の識別の結果を示す。続く準備 2 で，コントロール構造の構築を行う。構築したコントロール構造は，STEP 2 の潜在原因の識別で用いるものと同じで，図 1 のような構造となる。

表１．ハザードおよび安全制約の識別

ハザード		安全制約
(1)	アクセルを開けた時にスロットルが開かない	アクセルを開けた時はスロットルが開く
(2)	アクセルを閉じた時にスロットルが閉じない	アクセルを閉じた時はスロットルが閉じる
(3)	アクセルを開けているのにスロットルが閉じる	アクセルを開けているときにスロットルは閉じない
(4)	アクセルを閉じているのにスロットルが開く	アクセルを閉じているときにスロットルは開かない

STEP 1 では，前章で示した制御アクションに関する 4 つの不適切な状態をガイドとして，不適切な制御アクションを識別する。本アイテムの制御アクションは，スロットルを開ける指示およびスロットルを閉じる指示である。不適切な制御アクションの識別結果を表 2 に示す。

表２．不適切な制御アクションの識別

制御アクション	安全のための制御アクションが設置されていない	ハザードにつながる安全ではない制御アクションが設置されている	タイミングが遅すぎる，早すぎる，または定められた順序に設置されていない	制御アクションが設置されているが，すぐに止まる，もしくは適用が長すぎる
スロットルを開ける指示	アクセルを開けたのに，スロットルを開ける指示が行われなかった	アクセルを閉じたのに，スロットルを開ける指示が行われた	アクセルを開けたのに，スロットルを開ける指示がすぐに行われない	アクセルを開けているのに，スロットルを開ける指示が止まった
スロットルを閉じる指示	アクセルを閉じたのに，スロットルを閉じる指示が行われなかった	アクセルを開けたのに，スロットルを閉じる指示が行われた	アクセルを閉じたのに，スロットルを閉じる指示がすぐに行われない	アクセルを閉じているのに，スロットルを閉じる指示が止まった

次に STEP 2 の潜在原因の識別を実施する。今回識別したアイテムの，潜在原因の識別結果を図 1 に示す。ここで識別された潜在原因に対し，安全目標を達成するための安全方策を検討することができる。

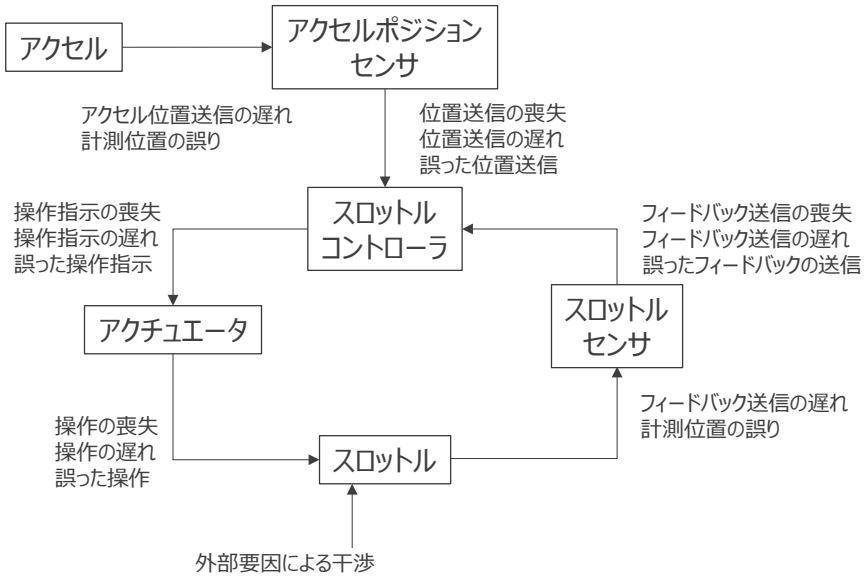

図１　潜在原因の識別

４．まとめ

システム理論に基づく安全性解析手法である STAMP と，その適用事例について調査研究を行った。従来から用いられている FTA や FMEA に比べ，STAMP を用いることで，ソフトウェアも含めたシステムのハザードにつながる不適切な制御アクションの潜在原因の識別が，短時間かつ高い網羅性で行えることが期待できる。鉄道システムへの適用事例はまだほとんどないが，高安全な鉄道システムの開発にとって，STAMP は有効な解析手法になり得ると考える。

以上

参考文献

(1) IEC 62278 (Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)), 2002.

(2) Nancy G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, 2011.

(3) 八山 幸司，米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状（前編），IPA ニューヨークだより，2014.