日本における STAMP/STPA への取り組みと鉄道システムへの適用に関する調査研究

日本大学　理工学部　応用情報工学科　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。このようなシステムの安全性解析には、従来から広く用いられている FTA（Fault Tree Analysis）や FMEA（Failure Mode and Effect Analysis）だけでは限界がある。

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アクシデントモデルとして、システム思考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 [(1)]。そして、STAMP モデルを前提としたハザード要因を分析する安全性解析手法である STPA（STAMP based Process Analysis）が活用されつつある。

これまで、日本における STAMP/STPA への理解および活用はあまり進んでいなかった。しかし、独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア高信頼化センター（SEC）は、STAMP/STPA の重要性をいち早く認識し、2015 年度に新設したシステム安全性解析手法 WG による報告書を 2016 年 4 月に発行している [(2)]。また、IPA は九州大学らと共催し、2016 年 12 月に「第 1 回 STAMP ワークショップ in Japan」を開催している。

本調査研究では、上記の日本における STAMP/STPA への取り組みおよび鉄道システムへの適用状況について調査することで、その有効性と課題に関する知見を得ることを目的とする。

２．日本における STAMP/STPA への取り組み

日本における STAMP/STPA への取り組みとして、IPA/SEC による報告書および日本で開催された STAMP ワークショップについて概説する。

２．１　IPA/SEC による報告書

IPA/SEC は、2016 年 4 月にシステム安全性解析手法 WG の報告書として「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～」を公開した [(2)]。本報告書は、日本における STAMP/STPA の入門書として、おそらく最初のものと思われる。

本報告書は総ページ数 57 ページの小冊子で、現在のところ IPA の Web ページから無償でダウンロードできる [(2)]。STAMP の基本的な解説から、STPA の分析実施例など、STAMP 初学者にとって有益な情報がコンパクトにまとめられている。表 1 に、本報告書の目次（章のみ）を示す。

表１．「はじめての STAMP/STPA」の目次

1.	STAMP 解説
2.	STPA の手順（全体説明）
3.	対象システム概要
4.	STPA 分析実施例の説明
5.	Advanced Technic
6.	エンタープライズ系システムでの STAMP 適用
7.	まとめ

第 1 章および第 2 章は、STAMP の解説と STPA の手順が書かれている。これらの解説は日本の STAMP/STPA のエキスパートにより書かれており、少ない紙面にもかかわらず、わかりやすい解説がなされている。特に STPA を実施するための手順、すなわち、Step0 準備 1：アクシデント、ハザード、安全制約の識別、Step0 準備 2:コントロールストラクチャーの構築、Step1:安全でないコントロールアクションの抽出、Step 2：非安全なコントロールの原因の特定について簡潔に説明されている。この説明に従えば、具体的なシステムを対象に、すぐにでも STPA を実施できそうな印象である。

第 3 章および第 4 章は、STPA の適用事例研究が述べられている。ここでは具体的対象として、列車制御システムを構成する踏切制御システムを取り上げている。第 3 章で、対象システムである単線の駅中間踏切制御システムの概要および要求仕様を述べ、第 4 章でこの装置に対する STPA 分析を実施している。

第5章は、Advanced Technic が書かれている。まず、STAMP を支援するツールである XSTAMPP（An eXtensible STAMP Platform）が紹介されている。XSTAMPP は Java でプログラムされており、3 つのプラグインにより STPA などの基本的な支援をする機能を持つ。第 3 章で述べられた踏切制御システムを例に、XSTAMPP の具体的な使用方法が、画像を使って丁寧に説明されている。さらに、SysML（Systems Modeling Language）記述からの STAMP 構築や、状態遷移図の活用についても述べられている。

第 6 章は、エンタープライズ系システムへの STAMP の適用について書かれている。エンタープライズ系システムには、金融システムや行政情報システム、情報通信システム、交通制御システムなどが含まれ、システム障害によりサービスが継続不可になった場合、その影響は非常に大きいものとなる。

さらに IPA/SEC は、この報告書の続編として、2017 年 3 月に「はじめての STAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～」も発行している [(3)]

２．２　第１回 STAMP ワークショップ in Japan

IPA は九州大学らと共催し、2016 年 12 月 5 日～ 7 日の 3 日間、九州大学稲盛財団記念館および九州大学西新プラザにおいて、「第 1 回 STAMP ワークショップ in Japan」を開催した。開催者の報告では、約 130 名もの講演者および参加者があり、日本における STAMP への関心の高さが伺える。筆者も聴講者として参加した。

3 日間の開催期間中に、3 件の Keynote speech、6 件の招待講演、そして 16 件の一般講演が行われた。これらの講演資料は、現在のところ IPA の Web ページから無償でダウンロードできる [(4)]。

3 件の Keynote speech はすべて MIT の Dr. John Thomas によるもので、それらは「STPA チュートリアル（初級）」、「STPA チュートリアル（中級）」、「STPA 研究事例」である。STPA チュートリアルでは、簡単な化学プラントシステムを例に、参加者が実際に STPA の各ステップを実体験することで、理解を深めることができた。「STPA 研究事例」では、車の自動駐車アシストシステムについて解説された。

6 件の招待講演は、大学および企業からの講師により行われ、STAMP のみならず、今後の安全性解析として期待されるレジリエンスエンジニアリングについての講演もあった。

次に 16 件の一般講演について述べる。講演者の所属の内訳は、大学等の教育機関（8 件）、一般企業（6 件）、IPA（2 件）であった。鉄道関係では、鉄道事業者および信号メーカからそれぞれ 1 件の講演があった。16 件のうち 2 件が鉄道関係者からの発表であり、鉄道システムに対する STAMP/STPA の適用への関心の高さが伺える。各講演の対象とするシステムの内訳を表 2 に示す。対象システムは様々であるが、鉄道システムを対象とした講演が 3 件あった。

一般講演の内容を調査した。すべての講演において、具体的システムへの STAMP/STPA の試行がなされていた（16 件）。これらの中には、FTA など従来手法との比較したものが含まれる（3 件）。さらに、STAMP/STPA を発展させる内容として、ツール開発に関するもの（1 件）や拡張に関するもの（4 件）が発表された。拡張については、STAMP/STPA での定量的評価を試みたもの（1 件）、STPA の Step1 で行うハザードにつながるコントロールアクションの識別支援に関するもの（1 件）、Step2 で行うハザード要因の抽出支援やヒントワードの提案に関するもの（2 件）があった。

表２． 一般講演で対象とされたシステムの内訳

対象システム	講演件数
農業用システム	2
通信ネットワークシステム	2
複雑システム（人，組織，機械，環境を含んだシステム）	2
ET ロボコン用ロボット	3
水中パーソナルビークル	2
健康増進システム	1
エンタープライズ系システム	1
鉄道システム	3

３．STAMP/STPA の鉄道システムへの適用

これまでのところ、日本において STAMP/STPA を鉄道システムに適用した事例はほとんど見当たらない。本章では、IPA/SEC の公開した「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～」と、「第 1 回 STAMP ワークショップ in Japan」での適用事例について概説する。

「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～」では、単線の駅中間踏切制御装置を対象システムとしている。上り下り2つの警報開始センサー、踏切近傍に設置された警報終始センサーおよび踏切制御装置により構成されたシステムについて、踏切制御装置が遮断機等に対して警報開始命令を正しく指示できること、異常時でも安全に制御できることを検証している。STPAの各ステップに従った詳細な説明がなされ､最終ステップとして対策のまとめまで示されている。また、随所に「勘所」として重要事項がまとめられており、実際に本手法を適用する場合に有益である。

阿満は、踏切制御機能を司る、駅構内論理装置に対してSTAMP/STPAを適用した事例を発表している[(5)]。駅構内は多くの列車が行き交うので、そこでの踏切制御は複雑となる。適用の結果、状態遷移の明確化や連動装置と踏切制御装置のより厳密な情報交換の必要性が明らかになった点など、本手法が有効であると結論づけている。

高田は、電子連動装置に用いられるFS-CPUブロックに対してSTAMP/STPAを適用した事例を発表している[(6)]。FS-SCPUブロックは、電子連動装置のみならず、列車制御システムの各装置に用いられる重要なブロックである。ここでは、鉄道の国際規格であるRAMS規格への対応も視野に、STAMP/STPAでの定量的評価についても述べている。

４．まとめ

日本におけるSTAMP/STPAへの取り組みと、鉄道システムへの適用状況について調査研究を行った。IPA/SECによるSTAMP/STPAの入門書の公開や、第1回STAMPワークショップ in Japanの開催など、日本においてもSTAMP/STPAの関心が高まりつつある。また、鉄道システムへの本手法の適用も事例が出始めている。今後、本手法の適用事例が増え、その有効性と課題が明確になることが期待される。また、ツール開発や、手法の拡張の研究を推進することも必要である。さらに、海外での取り組みも調査する必要があると考える。

以上

参考文献

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

(2) システム安全性解析手法WG，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～，IPA，Ver.1.0，2016.4.
（http://www.ipa.go.jp/sec/reports/20160428.html）

(3) システム安全性・信頼性分析手法WG，はじめてのSTAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～，IPA，Ver.1.0，2017.3.
（http://www.ipa.go.jp/sec/reports/20170324.html）

(4) 第1回STAMPワークショップ in Japan
（http://www.ipa.go.jp/sec/events/20161205.html#001）

(5) 阿満利仁, 駅構内論理装置の踏切制御機能仕様に対する STAMP/STPA 解析, 第 1 回 STAMP ワークショップ in Japan
(http://www.ipa.go.jp/files/000056631.pdf)
(6) 高田哲也, STAMP 解析での定量的評価と STAMP 解析の開発プロセスにおける適用段階, 第 1 回 STAMP ワークショップ in Japan
(http://www.ipa.go.jp/files/000056632.pdf)