米国における STAMP（システム理論に基づく事故モデル）研究の最新の動向

八山　幸司
JETRO/IPA New York

1　はじめに

ソフトウェアを使ったシステムの発達は拡大の一途を辿っており、人々の目に見えない場所で生活を支えるあらゆるシステムがコンピューターとソフトウェアによって構成されてきている。その一方で、自動運転システムや人工知能など人間に代わって知的な作業を行うシステムについては、人々がどこまで安全性が担保されているかを確認することも難しくなってきている。このような情報化社会・高度システム化社会に対応する形で生まれたのが新しい事故モデル STAMP（Systems Theoretic Accident Model and Processes／システム理論に基づく事故モデル）であり、従来の事故モデルだけでは対応できない最先端のシステムに対する有効性が認められてきたことで、多くの企業や研究機関から注目を集めている。より効率的かつ確実に安全性を実現しようとする企業や研究者の努力により、STAMP を使った手法は更なる発達を遂げており、実用的な事故モデルとして活用が広まっている。ニューヨークだよりでは以前、2014 年 5 月号と 6 月号で STAMP の研究について紹介を行ったが、今号では、2015 年 3 月に行われた STAMP ワークショップで発表された最新の研究結果や活用事例について紹介することで、その後の STAMP 研究の進捗をレポートしたい。

最初に、STAMP の概要や分析に必要なツールについて紹介を行う（STAMP の概要については昨年のニューヨークだより 5 月号でも紹介しているので、簡単におさらい）。STAMP はソフトウェア集約的なシステム（Software Intensive Systems）[1]に対応する新しい事故モデルとして注目を集めており、2015 年 3 月にマサチューセッツ工科大学（Massachusetts Institute of Technology：MIT）で行われた STAMP ワークショップでは、米連邦政府の研究機関や世界各地の大学機関から研究発表が行われた。STAMP のアイデアを基にしたツールも洗練されてきており、ハザード分析を行う STPA（System Theoretic Process Analysis）などは事故シナリオを特定するための一歩進んだ手法を提示している。また、システムのコンセプトや要件定義の段階からハザード分析を行う STECA（System Theoretic Early Concept Analysis）も新しく発表されたことで、あらゆる段階におけるハザード分析が可能となってきている。

次に STAMP の活用事例について紹介する。先進技術における代表的な活用例は、米空軍の無人航空機の運用に関するハザード分析であり、具体的な設計に至っていない無人航空機を運用する際に、認知システム工学と STPA を併用した分析を行っている。自動車設計への応用では、信頼設計から安全設計へと移行するために、従来の製品設計プロセスに STPA を組み込んだ分析となっている。蓄電池システムで発生した事故分析では、様々な組織における改善策の提案につながっている。この他、医療 IT プラットフォームの構築や、スーパーコンピューターの開発プロジェクトに STPA を使ったハザード分析の事例を取り上げる。社会システムに関しての活用事例では、医療現場における安全に向けた活用状況、巨大プロジェクトにおける新しい活用について紹介する。さらに、STAMP の研究によって浮かび上がってきた、今後必要となる取り組みや課題についても紹介していく。

これに続いて STPA のハザード分析をサポートするアプリケーションを取り上げ、XSTAMPP と Tool-Based STPA について紹介する。ドイツのシュトゥットガルト大学で開発されている XSTAMPP は、STPA を効率的に行うためのアプリケーションとなっており、プラグインの追加やオープンソースでの提供など様々

[1] ソフトウェア集約的なシステム（software-intensive system）とは、組み込まれたソフトウェアがシステム全体の設計、構造、配置、進化に影響に及ぼしているシステムを指す。

な取り組みが進められている。Tool-Based STPA もハザード分析を可能な限り自動化するためのアプリケーションとなっており、開発のためのアイデアが発表されている。

最後に、STAMP を使った新しい取り組みと、今後の課題について紹介する。具体的には、GM 社と MIT からの研究発表をもとに、STPA を反復することで確実なハザード分析を行う手法について取り上げる。いずれも単にハザード分析を行うだけでなく、より効率的であらゆるシステムの範囲に対応したハザード分析を行っている。また、STAMP の実用化が進むにつれて新しい課題も出てきており、組織構造や運用の変化に応じた STPA の活用や、STPA を使ったハザード分析から改善策を得られなかったケースについて取り上げていく。

STAMP は様々な分野へと広がっているだけでなく、その活用や手法はより実践的なものとなってきている。今号では STAMP の新しい情報を中心に紹介しているため、STAMP の基礎や過去の事例についてはニューヨークだより 2014 年 5 月号と 6 月号を参照していただきたい。2015 年 3 月に行われた STAMP ワークショップでは、13 か国から 260 人以上の研究者や技術者の登録があり、日本からも多数の参加が見られた。世界が注目する新しい事故モデルが、日本の最先端技術と社会システムにどのような影響をもたらすか見ていきたい。

図表 1：STAMP ワークショップの様子

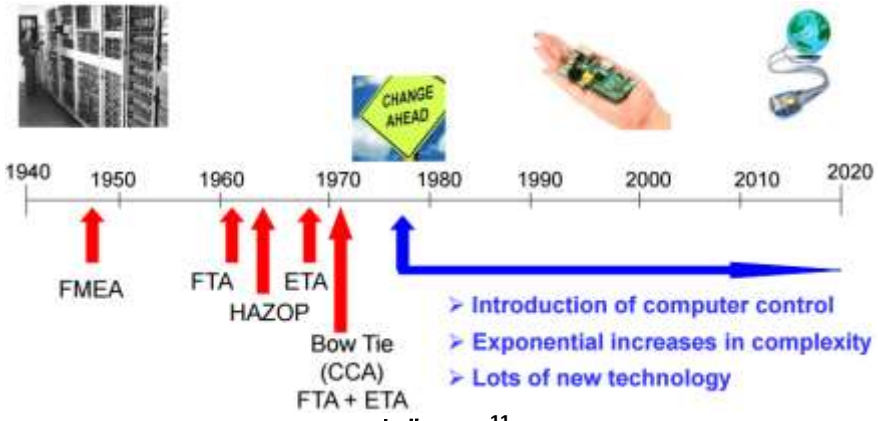
2　STAMP の概要

（1） STAMP とは

システム理論を用いた事故モデル STAMP（Systems Theoretic Accident Model and Processes）は、ソフトウェア集約的なシステム（Software Intensive Systems）[2]に対応した新しい事故モデルとして、多くの企業や研究者から注目を集めている。STAMP とは、マサチューセッツ工科大学（Massachusetts Institute of Technology：MIT）のナンシー・レブソン教授（Nancy Leveson）により考案された事故モデルであり、システムのメカニズム、テクノロジー、ヒューマンエラー、プロジェクト間の連携ミスなど、従来の事故モデルでは見つけることが難しかったシステム全体の設計に起因する事故原因を特定しやすくなっていることが特徴となっている[3]。

スイスチーズモデルやフォルトツリー解析（Fault Tree Analysis：FTA）[4]といった従来の事故モデルでは、機器の故障などによる事故を想定しているため、冗長性を持たせようと過剰設計になりやすく、システム全体の設計に潜む事故要因を特定することが難しいという欠点あった[5]。このため、STAMP ではシステムを構成するコンポーネント[6]間の相互作用やシステム間の連携を分析することにフォーカスしており、システムのあらゆる段階における事故要因の特定をより確実に行うことができるようになっている。図表 2 は、様々な事故モデルの登場を時系列でまとめたものである。FMEA[7]、FTA、HAZOP[8]、ETA[9]、Bowtie[10]といった代表的な事故モデルの多くが、コンピューターが発達する 1980 年代より前に登場していることがわかる。

図表 2：事故モデルの進化



出典：MIT[11]

[2] ソフトウェア集約的なシステム（software-intensive system）とは、組み込まれたソフトウェアがシステム全体の設計、構造、配置、進化に影響に及ぼしているシステムを指す。
[3] http://mitpress.mit.edu/books/engineering-safer-world p.389
[4] フォルトツリー解析（Fault Tree Analysis：FTA）とは事故分析手法の一つで、イベントごとに枝分かれした図を描いて、事故の原因を特定する手法のこと。
[5] http://mitpress.mit.edu/books/engineering-safer-world p.102
http://mitpress.mit.edu/books/engineering-safer-world p.28
[6] ここで指すコンポーネントとは、コンピューター、機械、オペレーター、組織など、何らかの要素のこと。各コンポーネントは指示を出す、指示を受けることで何らかの行動を起こす、またはフィードバックを返すなど、各々の役割を持っている。
[7] 故障モード影響解析（Failure Mode and Effect Analysis：FMEA）は、故障のメカニズムを研究しておくことで、潜在的な故障要因を特定する解析手法。
[8] HAZOP（Hazard and Operability Studies）は、設計や運用におけるハザード分析の手法。
[9] 事象の木解析（Event Tree Analysis）は、FTA の手法に事故が発生する確率を加えたハザード分析の手法。
[10] Bowtie（蝶ネクタイ）法は、想定される事故を中心に原因と結果を左右に配置して蝶ネクタイのような図を使用するハザード分析の手法。
[11] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STAMP-Tutorial.pdf

現在、STAMP をより効果的に活用するための研究が様々な機関や研究者によって進められている。2015 年 3 月に MIT で行われた第 4 回 STAMP ワークショップでは、NASA、ローレンス・リバモア国立研究所（Lawrence Livermore National Laboratory）、サンディア国立研究所（Sandia National Laboratories）、米空軍（U.S. Air Force）など、米連邦政府の最先端の研究機関が研究内容を発表しており、企業からも GM 社、Boeing 社、日産自動車などの参加があった。その他、ドイツのシュトゥットガルト大学（University of Stuttgart）、スイスのチューリッヒ大学（University of Zurich）、オーストラリアのグリフィス大学（Griffith University）など、世界各地の大学の研究機関が STAMP を使った研究内容を発表した。

また、ブラジルといった新興国の研究機関も積極的に STAMP の研究に取り組んでおり、STAMP への注目は今や世界規模になっている[12]。2015 年 10 月には、オランダのアムステルダム大学（University of Amsterdam）で 3 回目となるヨーロッパ STAMP ワークショップが開催される予定となっており、STAMP の研究と活用が世界中へ広まっていることは間違いない[13]。図表 3 はヨーロッパ STAMP ワークショップの案内となっている。

図表 3：ヨーロッパ STAMP ワークショップの案内

出典：MIT[14]

（2） STAMP の事故モデルを使ったツール

a. STPA

STAMP のアイデアに基づき様々なツールの研究開発が進められており、今回のワークショップでも MIT の研究室からハザード分析ツールに関する詳しい手法について発表があった。事故要因（ハザード）を事故が起きる前に特定するハザード分析は、STPA（System Theoretic Process Analysis）と呼ばれるハザード分析ツールをもって行われるが、STPA では事故につながるハザードの特定だけでなく、事故が起きるメカニ

[12] http://psas.scripts.mit.edu/home/stpa2015/2015-stamp-workshop-presentations/
[13] http://www.amsterdamuas.com/car-technology/about-the-centre-of-applied-research/calendar/calendar/calendar/content/folder/workshops/2015/10/3rd-european-stamp-workshop.html
[14] http://www.amsterdamuas.com/car-technology/about-the-centre-of-applied-research/calendar/calendar/calendar/content/folder/workshops/2015/10/3rd-european-stamp-workshop.html

ズムを解明することで事故のシナリオそのものを見つけ出すことができる。STPA のハザード分析のプロセスは、以下の 4 つの段階に分かれている[15]。

- 準備 1: アクシデントとハザードの設定
- 準備 2: コントロールストラクチャの構築
- STPA Step1: 安全でないコントロールアクション（Unsafe control action）の識別
- STPA Step2: 潜在原因（Causal factor）の識別

準備 1: アクシデントとハザードの設定

ここで言う**アクシデント**とは、予期しない事象により発生する人命や設備の喪失、環境汚染、プロジェクトの失敗など最も避ける必要のある事故のことを指す。**ハザード**とは、状況や環境の変化により事故の発生（アクシデント）につながる恐れのある状態のことである。アクシデントが災害などの制御不可能な事象を含む一方で、ハザードはシステムの設計などで制御や予防することが可能なものを指している[16]。

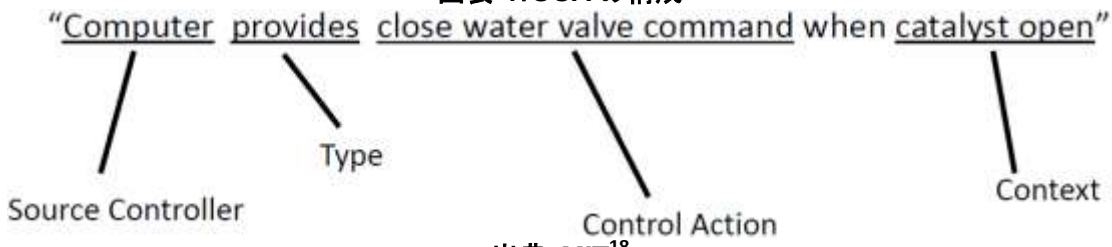
準備 2: コントロールストラクチャの構築

コントロールストラクチャとは、物理的な設計図ではなく機能動作を示した設計図となっている。コントロールストラクチャの作成には、システムを構成要素として**コントローラー**（Controller）と呼ばれるコンポーネントを用意し、制御する側からの制御指示となる**コントロールアクション**（Control action）と、制御される側からの**フィードバック**（Feedback）を示した矢印を各コンポーネント間で結んでいくことで、システム全体の機能動作を把握するための設計図を作成する仕組みとなっている。

STPA Step1: 安全でないコントロールアクション（Unsafe control action）の識別

安全でないコントロールアクション（Unsafe control action：**UCA**）とは、ハザードにつながる恐れのある不適切で安全でないコントロールアクションのことである[17]。UCA は、①制御元となるコントローラー（Source controller）、②制御の種類（Type）、③コントロールアクション（Control action）、④動作時の状況（Context）により構成されている。なお、制御の種類（Type）について、「コントロールアクションが設置されていない」、「安全ではないコントロールアクションが設置されている」、「コントロール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」、「コントロールアクションがすぐに止まる、もしくは適用が長すぎる」の 4 つに分類される。図表 4 はこの構成状況を示したものである。

図表 4：UCA の構成



出典：MIT[18]

UCA はハザードを防止するためのルールとなる**安全制約**（Safety constraint）の作成につながるため、UCA からハザードを判断するためのトレーサビリティー（Traceability）の確保なども必要となる。トレーサビリティーの確保には、ハザードごとに UCA の表を作成するか、UCA の後尾に"[H-1]"といったハザードの種類を示しておくなどの方法がある[19]。

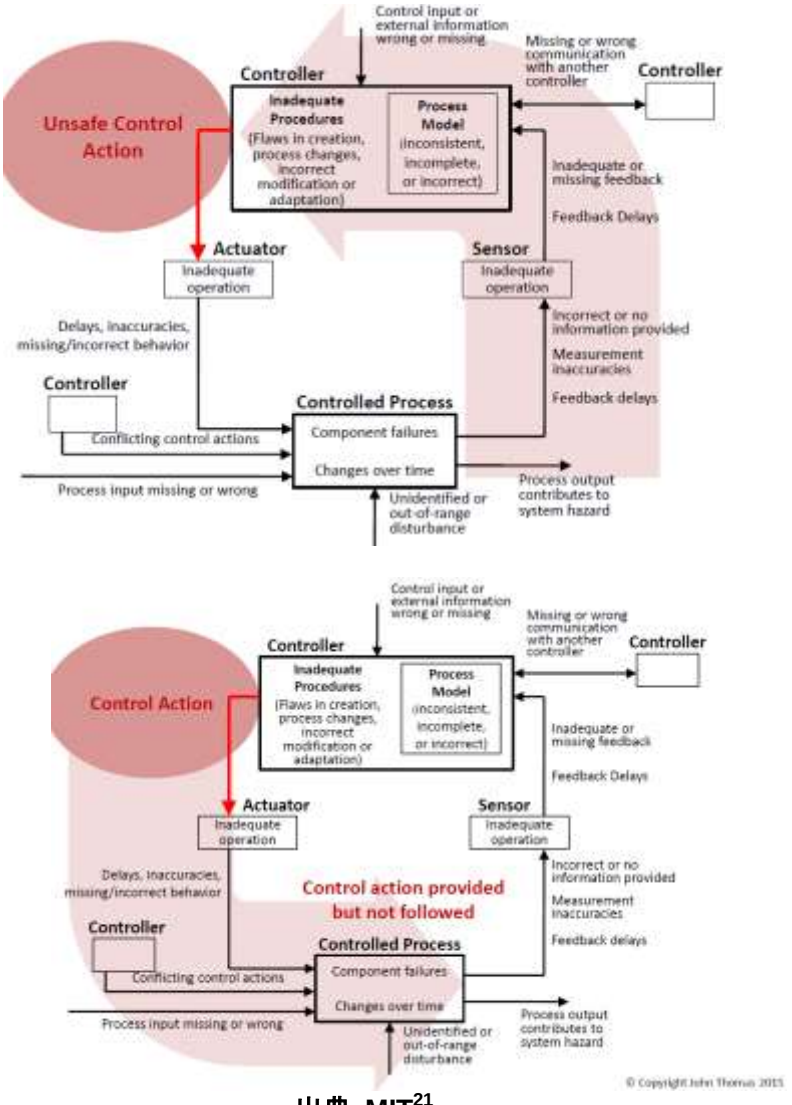
[15] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf
[16] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf
[17] http://mitpress.mit.edu/books/engineering-safer-world p.217
[18] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf
[19] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf

STPA Step2: 潜在原因(Causal factor)の識別

最後のステップが、事故の要因となる**潜在原因**(Causal Factors)の特定であり、これをもって事故シナリオの作成が実現する。潜在原因と事故シナリオには大きく分けて、「UCA を引き起こす原因の特定」と「コントロールアクションが(次の動作に)正しく続いていない」の 2 種類がある。1 つ目の「UCA を引き起こす原因の特定」は、UCA の発生より前の段階に着目することで原因を特定するものである。2 つ目の「コントロールアクションが(次の動作に)正しく続いていない」については、機器が正常に動作しコントロールアクションが正しく行われていても、システムの設計ミスなどにより次の動作につながっていない状態となっている場合を指しており、特定のコントロールアクションから後のプロセスを確認していくことで原因を特定する形となる。

図表 5 にある 2 種類の図は、シンプルなコントロールストラクチャ上での潜在原因と事故シナリオの特定手順を示したものである。上の図が「UCA を引き起こす原因の特定」で、下の図が「コントロールアクションが(次の動作に)正しく続いていない」ことを示している[20]。

図表 5:潜在原因と事故シナリオの特定



出典:MIT[21]

[20] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf
[21] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf

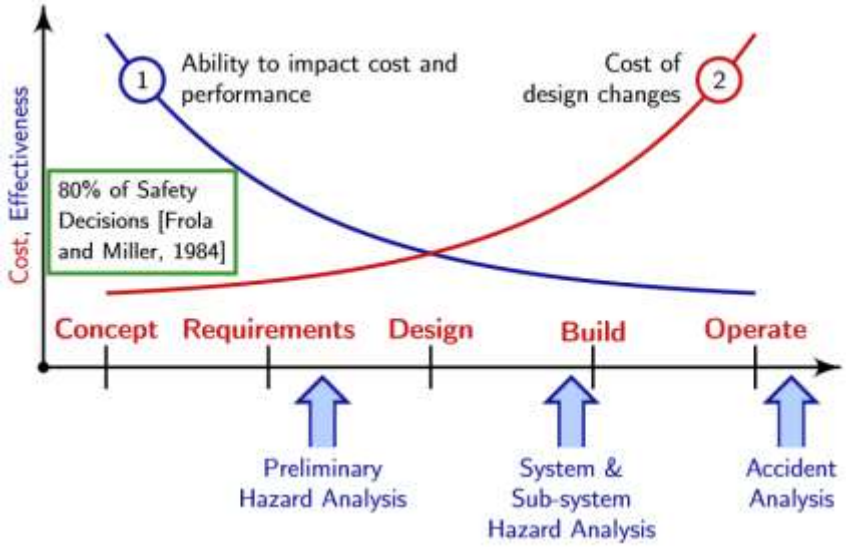
b. CAST

CAST（Causal Analysis using System Theory）とは、STAMP を使った事故分析ツールであり、事故後に検証と分析を行うためのものである。分析の手順は STPA とほぼ同じであるが、CAST では事故への直接的な要因そのものを追究すると同時に、システムがどのようにして事故へとつながったのかなど事故のメカニズムの追及を行う点が特徴となっている。例えば、事故の直接的な要因がヒューマンエラーによるものであっても、間違いにつながりやすい機器の配置やデザイン、複雑な生産工程、無理な生産目標によるプレッシャーなどヒューマンエラーにつながるシステム上の問題についても分析する形となる。CAST では事故が起きた理由やプロセスを明確に説明することができるため、事故原因を特定できた後に事故は予測可能であったと考える「後知恵バイアス」を減らす役割もある[22]。

c. STECA（System Theoretic Early Concept Analysis）

STECA（System Theoretic Early Concept Analysis）とは、システムのコンセプト・要件を定義する段階から安全性を分析するツールのことである。STPA や CAST がシステム構築後を対象としている一方で、Cody Fleming 氏が考案した STECA は、システム設計段階の安全性を考えるのではなく、システムのコンセプト・要件を定義の段階から安全性について踏み込む点が特徴であり、システム設計前の段階から安全設計を組み込んでいくことで、システムが構築された後に発生する安全性の見直しや、システムの改修に必要なコストを削減することを狙っている。図表 6 は、システムの安全性にかかるコストを示したものとなっている。青いラインが安全性について取り組んだ際の効率を示しており、赤いラインが安全性にかかるコストとなっており、システム設計前から安全性に取り組むことがコスト面からも重要であることがわかる。

図表 6：システムの安全性にかかるコスト



出典：MIT[23]

[22] http://mitpress.mit.edu/books/engineering-safer-world p.349
[23] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STECA-Tutorial.pdf

3　STAMP の活用事例

（1）　先進技術における活用

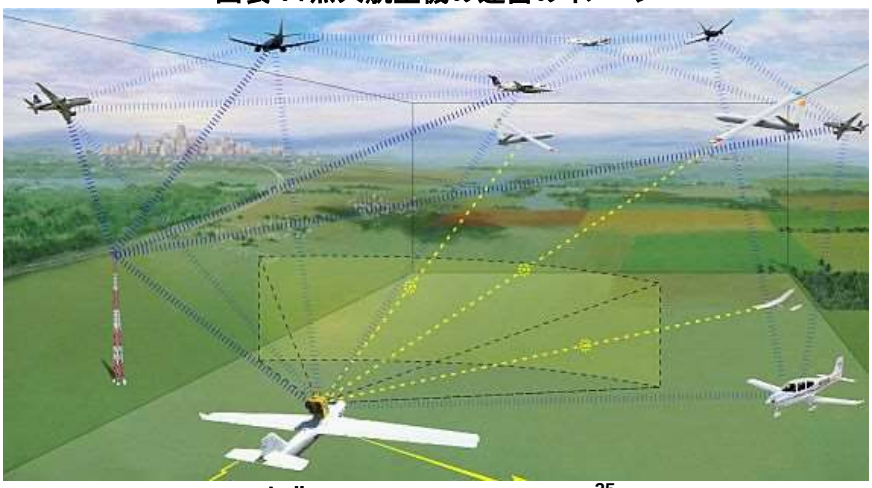
a.　無人航空機の運用における活用（地上や空中での衝突回避など）

先進技術分野では、無人航空機の運用における安全性の確保に向け、STPA を使いハザード分析を行うといった例がある。米空軍では米国内の空域で無人航空機を運用する上で様々な研究を行っており、地上や空中で他の航空機との衝突を避けるためのシステムの開発を進める上で生じる様々な問題をクリアするためにハザード分析を実施している。具体的には、同軍では自動回避システムが具体的な設計まで至っておらず、有効なデータも得られていないなど様々な課題を抱えていたほか、社会システムや技術的な課題が複雑に絡んでいるため、システム全体の設計に際して従来の安全分析の手法が適さないという問題にも直面していたため、認知システム工学（Cognitive Systems Engineering）の手法を応用し、抽象的なシステム要件からコントロールストラクチャの構築を行い、ハザード分析へとつなげている。

同軍による取り組みでは、まず抽象階層（Abstraction hierarchy）と呼ばれる手法を使い、システム全体から航空機までの各階層で安全性の確保に必要な要件を識別している。具体的には、システムを構成する要素（サブシステム）を規模に合わせて、米国内の空域、全米の航空管制システム、地方の航空管制システム、航空機の運航、航空機のシステムの 5 つに分類し、それぞれの機能を一覧にしたテーブルを作成している。次に、このテーブルから得られた結果を基にコントロールストラクチャの階層別にシステムを作り、各サブシステムの役割に基づいてコントロールストラクチャを構築する形となっている。

同軍が行った、STPA ベースのハザード分析からは、65 のシステムレベルの安全要件と自動回避システムに必要な 68 の安全証明の必要性が判明しており、具体化されていないシステムの設計要件から安全設計に必要な取り組みへとつなげている[24]。図表 7 は、無人航空機の運営のイメージを示したものである。

図表 7：無人航空機の運営のイメージ



出典：Military Aero Space [25]

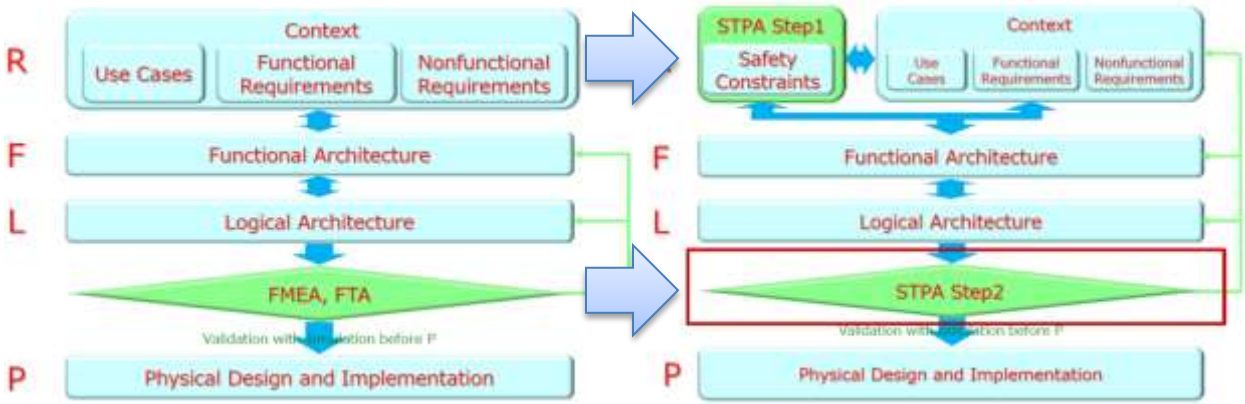
[24] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/04/Johnson_STAMP-2015-Presentation_Final.pdf
[25] http://www.militaryaerospace.com/articles/2014/06/uav-sense-avoid.html

b. 自動車の製品設計への活用（信頼設計から安全設計へ）

製品設計においては設計プロセスを新しく作り変えることは容易ではなく、STPA を組み込むという理由で製品設計プロセスを見直すことは非効率であることから、既存の設計プロセスに STPA を組み込もうという取り組みがある。例えば、日産自動車では RFLP アプローチと呼ばれる既存の製品設計プロセスの中に STPA を組み込むという取り組みを進めており、STAMP を実践活用しているという点で注目されている。日産自動車の RFLP アプローチとは、設計要件（Requirement）、機能設計（Functional architecture）、論理設計（Logical architecture）、物理設計（Physical design）という製品開発における 4 段階を示すものであり、これまでは FMEA や FTA といった設計信頼性検証プロセスを組み込んだものであった。従来の方法であれば、論理設計を行った後にサブシステムへと設計要件を渡し、サブシステムの設計と検証が完了した後にシステム全体の設計を完了することしか出来なかったが、STPA を RFLP アプローチに応用することで、設計の検証を行った後にサブシステムへと設計要件を渡すことが可能となっている。

同社の研究では、FMEA や FTA による「信頼設計」から STPA を使った「安全設計」へと移行することを目的としており、STPA Step1 を設計要件（Requirement）の中に配置し、論理設計の後に行われている検証プロセスに STPA Step2 を配置することで安全設計を実現している。同社は、設計要件に求められる機能要件と非機能要件は同じ様に安全制約が必要であるという考えに基づき、設計要件段階に STPA Step1 を配置するとともに、検証プロセスに STPA Step2 を配置することにより、サブシステムへ設計要件を渡す前の段階でシステムの設計を完了させているわけである[26]。図表 8 は RFLP モデルへの STPA の応用を示した図となっている[27]。

図表 8：RFLP アプローチへの STPA の応用



出典：MIT 資料を基に作成[28]

同社は製品設計プロセスへの STPA の組み込みにより、設計上の問題を原因とする潜在原因の特定に成功しており、STPA を応用した RFLP アプローチの有効性を証明している。また、同社の取り組みでは、システム設計の検証を行った後に効率的にサブシステムへと設計要件を移管できることもわかっている[29]。

c. 電池技術の事故分析のための活用（蓄電池システムの安全性）

米エネルギー省（Department of Energy：DOE）管轄下のサンディア国立研究所では、大型の蓄電池システムを運用する上で、STAMP を使った事故分析ツール CAST と STPA をベースに、安全性について分析している。電力網では様々な方法でエネルギーが貯蔵されるが、その中の 1 つであるフロー電池（流動電

[26] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/04/RFLP-with-STPA-by-Nissan.pdf
[27] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/04/RFLP-with-STPA-by-Nissan.pdf
[28] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/04/RFLP-with-STPA-by-Nissan.pdf
[29] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/04/RFLP-with-STPA-by-Nissan.pdf

池）は 2 種類の化学溶液を用いて電力を貯蔵するものとなっている[30]。サンディア国立研究所ではフロー電池を用いた蓄電池システムで発生した事故について CAST を使った事故分析を行っており、試運転を行っていたフロー電池の蓄電池システムにおいて様々な要因が重なったことにより、内容物である化学溶液が喪失した事例となっている。この事故では、タンクの内容物の漏れを検知するセンサーが取り外されていた上に、侵入した虫によって弁の 1 つがふさがれていたため、タンクの圧力が上昇して蓄電池システムへのダメージへとつながった[31]。

この事故の調査報告書では 3 つの改善案が出されているが、CAST を使った事故分析を使うことでさらに 9 つの改善案を見つけ出している。CAST の分析結果からは、DOE、蓄電池システムの管理者、システムの操作を行うオペレーター、蓄電池システムの製造を行うメーカーに対する改善案が策定されており、蓄電池システムを取り巻く各組織が持つリスクについて説明が出された。同研究所はさらに STPA を使って蓄電池システムのハザード分析を行っているが、STPA による分析からは、バッテリー本体は機能を請け負っているだけであり、バッテリー単体ではなく、バッテリーを含む蓄電池システム全体で安全性を担保する必要があるという結論に至っている[32]。図表 9 は、蓄電池システムにおける安全性について説明した図となっており、バッテリー本体ではなく蓄電池システム全体で安全性を考える必要があることを示したものである。

図表 9：蓄電池システムにおける安全性について

出典：MIT[33]

（2） ソフトウェアやスーパーコンピューターの開発における活用

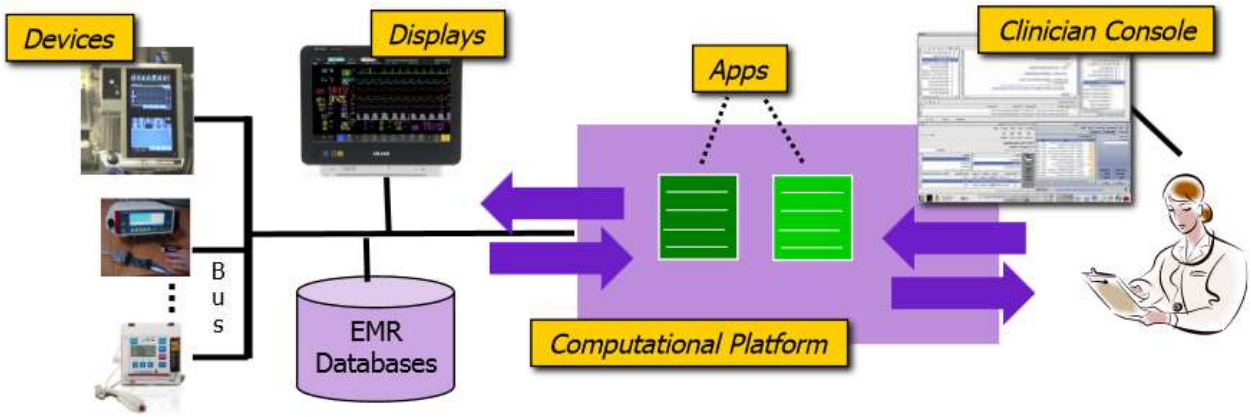
a. ソフトウェア開発における活用（医療 IT プラットフォームの例）

異なる医療機器間の相互運用を実現する医療 IT プラットフォームを構築するための取り組みでも、STPA が活用されている。具体的には、カンサス州立大学（Kansas State University）と FDA が医療機関内で使われる様々な医療機器を連携させデータを相互運用するためのプラットフォームを構築しているが、様々な医療機器で患者の医療データをリアルタイムで収集する上では、必要に応じて医療機器を制御するためのアプリケーションの開発が必要であることから、この開発過程で STPA をベースとしたハザード分析を行っている[34]。

図表 10 は、医療 IT プラットフォームを示したものである。紫で示された箇所が、ハザード分析が適用された開発アプリケーションとなっている。

[30] http://energystorage.org/energy-storage/storage-technology-comparisons/flow-batteries
[31] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Rosewater-Grid-Energy-Storage.pdf
[32] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Rosewater-Grid-Energy-Storage.pdf
[33] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Rosewater-Grid-Energy-Storage.pdf
[34] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Procter-Using-STPA-for-RM-in-Interoperable-Medical-Systems.pdf

図表 10：医療 IT プラットフォーム



出典：MIT[35]

アプリケーション開発に STPA ベースのハザード分析を適用しているのは、動作している医療機器からエラーが送られてきた場合、アプリケーションはエラーが何を起因とするものかを判断する必要があるからである。そのため、アプリケーションは原因となるソースコードの確認や、エラーによって患者への影響を調査するなど情報収集を行う仕組みとなっている。具体的には、コントロールストラクチャを使って設計されたシステムのアーキテクチャを基に情報が収集され、収集された情報はデータベースへと蓄積された上で、UCA のテーブルに反映される。これにより、システムがリアルタイムで UCA を判断し、ハザードにつながる情報を集めることが可能となる。この研究は現在も進められており、医療機器から送られた UCA 関連の情報が継続的に収集されている[36]。

b. スーパーコンピューター開発プロジェクトでの活用（核兵器シミュレーション用スーパーコンピューターの例）

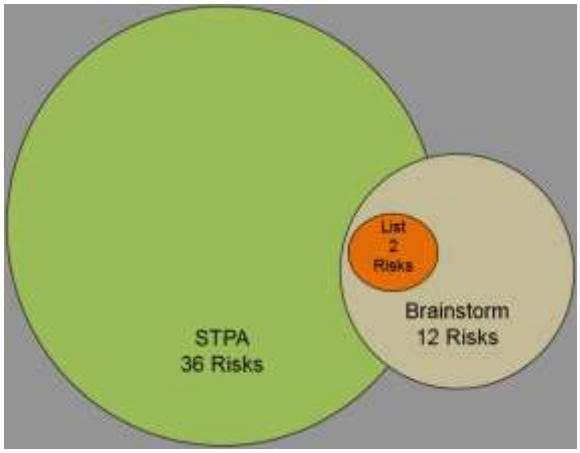
スーパーコンピューター分野についても、開発過程で様々な要因から発生する各種問題に対応する必要があるため、STPA を用いて開発のリスク要因を判別するという例が出てきている。例えば、DOE 傘下のローレンス・リバモア国立研究所では、先進シミュレーションおよびコンピューティング計画（Advanced Simulation and Computing：ASC）と呼ばれる核兵器のシミュレーションを目的としたスーパーコンピューターの開発を進めているが、スーパーコンピューターの開発には多大な労力が必要となるほか、予算や人材の不足、研究成果の不透明さ、核兵器開発への反対など多数の一般的な障壁があり、それ以外にもリスクが考えられることからハザード分析を行うことになった[37]。

同研究所では、米政府の政治的なリスク、連邦政府機関による計画上のリスク、ローレンス・リバモア国立研究所の運営上のリスク、スーパーコンピューターの開発上のリスク、運用上のリスクといった点をリスクとして想定した上でハザード分析を行っている。また、上部組織からの連絡が伝言ゲームによって不正確になっていくリスクや、別々の研究所から出されたアイデアが混ざり合って異なるアイデアとなってしまうリスクなども考慮して分析が進められた。ハザード分析の結果から、36 のリスクが見つけ出されたが、事前のブレインストーミングで想定されていた 12 のリスクのうち 10 個は STPA の分析結果の中に含まれていなかった。同研究所はプロジェクトに「リスクがあることを理解している」場合にはブレインストーミングも有効であるが、「認識していないリスクがあることを（残っていることを）わかっていない」場合に STPA が有効であると見て

[35] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Procter-Using-STPA-for-RM-in-Interoperable-Medical-Systems.pdf
[36] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Procter-Using-STPA-for-RM-in-Interoperable-Medical-Systems.pdf
[37] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Pope-STPA-for-Software-Quality-Org.pdf

いる[38]。図表 11 は ASC のハザード分析から見つかったリスクとなっている。左の図は STPA とブレインストーミングから見つかったリスクの数を表しており、右の図はどのような認識の時に STPA とブレインストーミングの分析が有効か示したものとなっている。

図表 11：ASC プロジェクトにおいてハザード分析により判明したリスク



- **Brainstorming**：リスクがあることを理解している
- **Lists**：認識していないリスクがあることを理解している
- **STPA & Brainstorm**：全部のリスクを認識しているかわからない
- **STPA**：認識していないリスクがあることを（残っていることを）わかっていない

出典：MIT[39]

（3） 社会システムを含めた活用

a. 医療現場における安全性確保に向けた活用（放射線治療における安全性）

様々な医療機器を扱う医療現場では、組織や連絡体制の不備から生まれる事故を防ぐ目的で、STPA を使ってハザード分析を行うという例がある。例えば、MIT とカリフォルニア大学サンディエゴ校（University of California, San Diego）は、放射線治療を安全に行うためにハザード分析を行っている。この例では、政府の監督機関から病院、医師、患者にいたるまでのコントロールストラクチャを構築した上で、その中から医療現場の安全に関係する、病院の管理者、治療プランを計画する医師、治療を行う技師などに焦点を当てる形でハザード分析が行われている[40]。

STPA Step1 の分析からは 85 の UCA が特定されており、例えば「診断画像や治療プランが提供されているにもかかわらず、技師が画像処理を行わない」という問題が特定されたという。これは、他の部署などで診断画像の撮影が完了しているにもかかわらず、技師の元へ画像が送られていないことに気づいていない場合や、画像が別の場所に送られている、画像が処理できないフォーマットになっているなどといったことに起因する問題である。そのため、この問題の判明後はソフトウェアと医療従事者の双方に対する改善案を策定できることとなった。具体的には、ソフトウェア面では撮影が行われた後に自動的に画像を処理するための状態にするなど、事故につながらないようにするための開発が行われており、医療現場ではチーム全体での情報共有の徹底や、技師が画像を送られてくるまで待機しないなどのルール作りなどが進められている[41]。

b. リスクマネジメントに向けた活用（石油パイプラインなど大規模プロジェクトにおける安全性）

石油パイプラインなどの大規模プロジェクトのコンサルティングを行う ILF コンサルティング社では、大規模プロジェクトにおけるハザード分析に STPA を活用している。同社では STPA を使ったハザード分析を数年前から行っており、2014 年の STAMP ワークショップではロシアのパイプラインプロジェクトにおけるハザー

[38] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Pope-STPA-for-Software-Quality-Org.pdf
[39] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Pope-STPA-for-Software-Quality-Org.pdf
[40] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Samost-Radiosurgery.pdf
[41] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Samost-Radiosurgery.pdf

ド分析が発表されている。今回のワークショップでは、STPA から得られたハザード分析に事故が発生するリスクを加味することで、事故が起こる可能性が高い事象に対してより詳しいリスクを分析するという研究が発表された。同社はこの研究により、35 件の高レベルの事故のリスクを 15 件にまで減らすことに成功しており、発生率の高い事故に対して集中的な安全管理を行えるようになっている[42]。

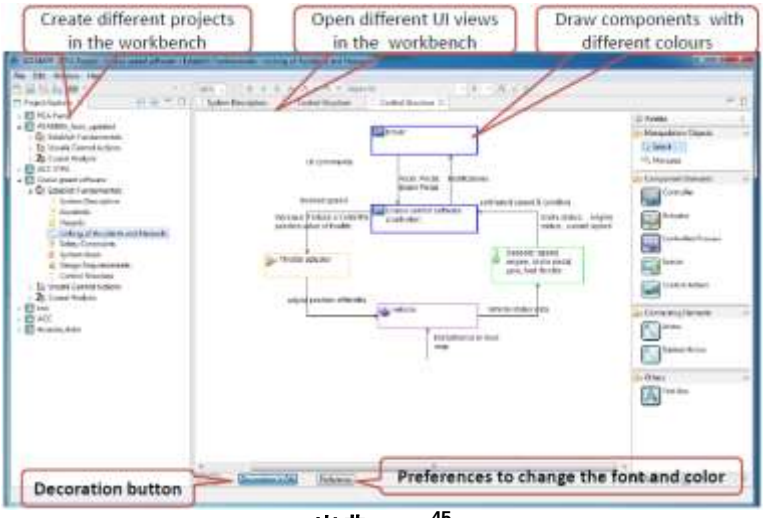
4 STPA ベースのハザード分析をサポートするツール

（1） XSTAMPP

STPA ベースのハザード分析を行うためのアプリケーションはこれまでも開発されていたが、最近ではこの分析プロセスを効率的かつ効果的に行える洗練したアプリケーションの開発が進められている。シュトゥットガルト大学で開発されているアプリケーション XSTAMPP（エックススタンプ）は最も先進的なアプリケーションの 1 つとなっており、ニューヨークだより 2014 年 5 月号の中でも紹介をした A-STPA の新しいバージョンとなっている。A-STPA についてはこれまでに 53 ヶ国から 3,000 近いダウンロードがあり、多くの研究者によって使われてきた。新バージョンの XSTAMPP では A-STPA の主要な機能を継承しつつ、様々な改良と機能追加が行われている[43]。

例えば、A-STPA では 1 つのプロジェクトしか扱うことができないシンプルな内容であったが、XSTAMPP では複数のプロジェクトを同時に扱うことが可能となっている。また、STPA のハザード分析をサポートするためのヘルプ機能や、作成したコントロールストラクチャをエクセル形式や画像として出力する機能も備えている。そして最大の特徴は、プラグインを作成するためのライブラリが提供されているため、XSTAMPP 用の追加機能を他の研究者も作成することができる点である。開発を進めているシュトゥットガルト大学の研究室では、CAST の事故分析を行う A-CAST プラグインや STPA の分析結果の検証を行う STPA verifier プラグインなどの開発を進めている[44]。図表 12 は、XSTAMPP のスクリーンショットである。

図表 12：XSTAMPP



出典：MIT[45]

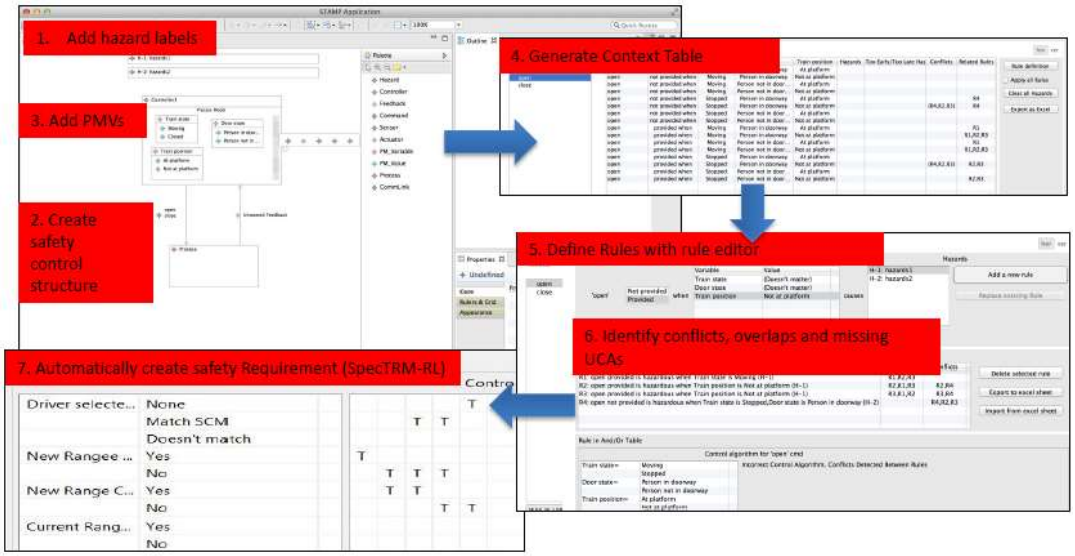
[42] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Pelegrin-STAMP-Project-Risk-Management.pdf
[43] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/XSTAMPP-An-eXtensible-STAMP-Platform-As-Tool-Support-for-Safety-Engineering.pdf
[44] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/XSTAMPP-An-eXtensible-STAMP-Platform-As-Tool-Support-for-Safety-Engineering.pdf
[45] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/XSTAMPP-An-eXtensible-STAMP-Platform-As-Tool-

XSTAMPP はシュトゥットガルト大学のウェブサイト上で公開されており、無料でダウンロードして使用することができるようになっている。また、XSTAMPP はオープンソースとなっているため、ソースコードも公開されている[46]。
ウェブサイト：http://www.iste.uni-stuttgart.de/se/werkzeuge/xstampp.html
ソースコード：http://sourceforge.net/projects/stampp/files/

（2） Tool-Based STPA

Tool-Based STPA は、MIT の John Thomas 氏により考案されたツールであり、STPA ベースのハザード分析プロセスの一部の自動化を目的としたものである。同ツールでは、STPA ベースのハザード分析プロセスを 11 段階に分け、ツールの使用によって主に STPA Step1 にあたる作業を自動化している。主な機能は、コントロールストラクチャとプロセスモデルから[47]コンテキストテーブル[48]の自動作成、コンテキストテーブル内のシステムのルールの矛盾の検知、安全のために必要な要件の生成などである。Tool-Based STPA は複数のツールを使った自動化となっており、例えば、安全要件の生成では SpecTRM と呼ばれるツールが使われている。Tool-Based STPA は John Thomas 氏により作成されているが、実験的に作られたものであるため、一般には公開されていない。そのため、ツールの動作や今後の課題などについてのみ発表されている[49]。図表 13 は Tool-Based STPA の動作を表したものである。

図表 13：Tool-Based STPA



出典：MIT[50]

Support-for-Safety-Engineering.pdf
[46] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/XSTAMPP-An-eXtensible-STAMP-Platform-As-Tool-Support-for-Safety-Engineering.pdf
[47] コントローラー内でコントロールアクションを決定する。ソフトウェアのアルゴリズムやオペレーターの意思決定などがある。
[48] システムが稼動した場合の機能の動作やシステムのプロセスを一覧にしたテーブル。
[49] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/Thomas-Suo-Tool-based-STPA-process.pdf
[50] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/Thomas-Suo-Tool-based-STPA-process.pdf

5　STAMP の新しい取り組みと課題

（1）　より確実なハザード分析への取り組み

a.　ハザード分析して設計変更した結果新たに生じる課題を、ハザード分析の反復で解消

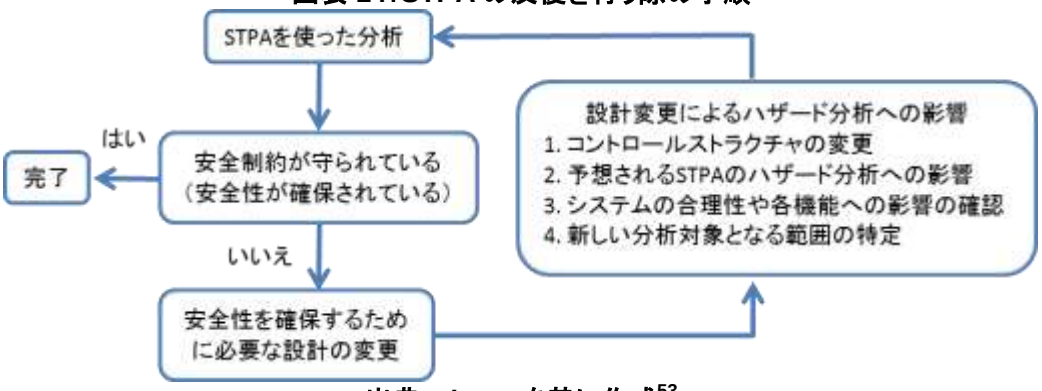
STPA ベースのハザード分析を繰り返し行い、システムの設計変更から生じる新たな UCA（安全でないコントロールアクション）について、新しい改善策が生み出されている。これまでの研究では、STPA のハザード分析からは様々な事故シナリオを見つけ出すことができるが、STPA の分析結果を基にシステムの修正を行った場合、新しい UCA が生まれるという問題があった。GM 社と MIT では、自動車の変速機を制御するシフトコントロールモジュールについて、STPA の分析を繰り返し行うことで、より確実なハザード分析を実現している。

これらによる取り組みでは、まずシステムレベルでのハザード分析を行い、システムの設計上に必要な修正を行っている。ただし、システムの設計修正により新しい UCA が発生している可能性があるため、コントロールストラクチャを詳細な物理レベルへと移行し、新たなハザード分析を行うという反復手順を踏んでいる。最初のシステムレベルのハザード分析は短時間で素早く行い、物理レベルのハザード分析で詳細な分析を注意深く行うというわけである。研究者によると、この STPA を繰り返し行う方法では、①システムを詳しく把握しコントロールストラクチャを洗練することができる、②コンセプト段階から詳細な設計まで効率的にハザード分析ができる、③抽象的な設計プロセスに対し詳細な安全要件を加えることができる、といったメリットがあるという[51]。

b.　効率的な STPA の反復の手法の研究

STPA を反復して行う場合、そのプロセスを一から繰り返すことは大きな手間であるとして、最小限のハザード分析を効率的に行えるようにするための研究が進められている。今回のワークショップで MIT の John Sgueglia 氏は、設計変更が STPA を繰り返し行うハザード分析プロセスにどのような影響を与えるかの研究を発表していた。同氏によると、STPA の反復には図表 14 のようなプロセスが発生するようになるという[52]。

図表 14：STPA の反復を行う際の手順



出典：vimeo を基に作成[53]

同氏は自動車のシフトコントロールモジュールを例に取り、設計変更によるハザード分析への影響と効率的なハザード分析の反復について説明した。この自動車のシフトコントロールモジュールの例では、STPA の

[51] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Sundaram-Iterative-Application-for-GM.pdf
[52] https://vimeo.com/album/3369082/video/123521943
[53] https://vimeo.com/album/3369082/video/123521943

ハザード分析結果を基に、車体からシフトコントロールモジュールへの変速機のポジション（ギアの状態）のフィードバックの追加、シフトコントロールモジュール上のアルゴリズムの変更が行われる形となるが、システム設計が変更されているため、新たな STPA のハザード分析を行うこととなる。

同氏の研究ではまず、STPA Step1 にどのような影響が出るかという点について、新しい機能からのコントロールアクションの発生、既存のコントロールアクションへの変更、新しい UCA が発生という点に焦点を当てている。STPA Step2 への影響ではコントロールループへの影響による新しい UCA の発生について焦点を当てている。同氏の研究からは、コントロールストラクチャの変更によって STPA Step1 への影響は出ていないものの、STPA Step2 への影響が考えられるため、次のハザード分析では STPA Step2 のみが実施される形となっていた[54]。図表 15 は設計変更によるハザード分析への影響をまとめたものとなっている。

図表 15：設計変更によるハザード分析への影響

STPA Step1	STPA Step2
• 新しい機能からコントロールアクションが発生しているか？ • 新しい機能によって既存のコントロールアクションに変更もしくは新しいコントロールアクションの発生があるか？ • 新しい UCA が発生しているか？ フィードバックの追加やシフトコントロールモジュールのアルゴリズムの変更によって、上記の項目に変化は発生していない。 ⇨ **前回の STPA Step1 がそのまま有効**	• システムの設計変更によって、どこのコントロールループに影響が出ているか？ フィードバックの変更によって、フィードバックを含んでいる UCA の事故シナリオに影響が出ている可能性がある。 シフトコントロールモジュールのアルゴリズムの変更によって、フィードバックのコントロールアクションが行われなかった時の事故シナリオに影響が出る可能性がある。 ⇨ **前回の STPA Step2 を見直して、新しい潜在原因と事故シナリオの特定を行う。**

出典：vimeo を基に作成[55]

次の段階は、システム設計変更によりシステムの様々な面へ影響が出る可能性があるため、合理的な判断や仮説を基に、予想される影響を考えていくというものである。自動車のシフトコントロールモジュールの場合、フィードバックの追加により様々なセンサーが変速機の状態を伝えるようになるため、どのように処理するかという問題が考えられるほか、アルゴリズムを変更するとドライバーが正しくギアの状態を把握できるかという懸念も生じる。これらの仮説を基に、ハザード分析の対象となる範囲を特定して新しいハザード分析を行うというのが、このステップである。今回の発表事例では、ドライバーとシフトコントロールモジュールの範囲について新しい STPA のハザード分析が行われていた[56]。

（2） STAMP の活用における課題

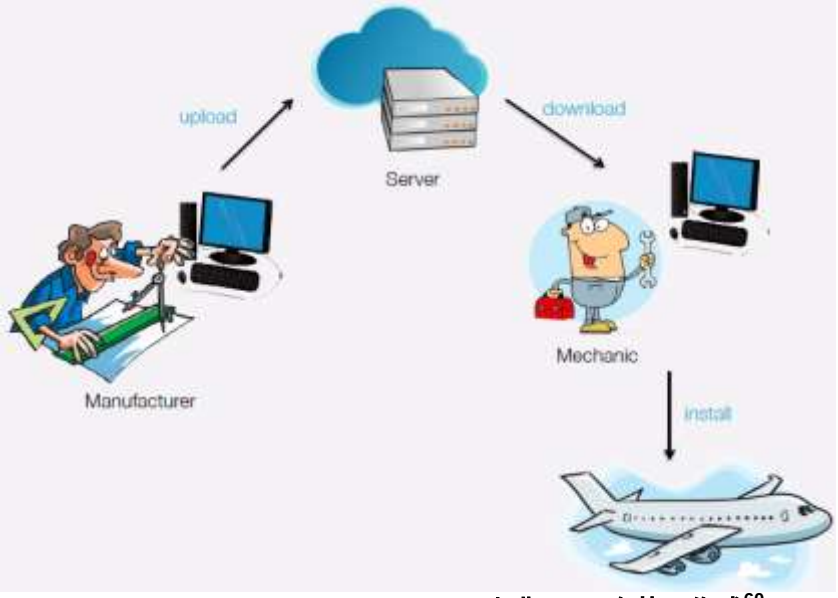
STAMP の研究や活用が様々な分野で進められる一方で、今後必要となる取り組みや課題も浮かび上がってきている。機械システムや組織の改革など、時間の経過とともに発生する機器の劣化や組織構造の変化について考慮していく必要があるため、MIT の研究からは、STPA のハザード分析から得られた結果を使った対応方法が発表されている。例えば、事故シナリオ基づいて行った性能監査（Performance audit）を、業務監査やシステム運用の基準として利用するといったことが提案されている。また、運用の変化に対応した

[54] https://vimeo.com/album/3369082/video/123521943
[55] https://vimeo.com/album/3369082/video/123521943
[56] https://vimeo.com/album/3369082/video/123521943

マネジメントのために STPA のハザード分析を使用するなど、システムの変化に応じて STPA を活用していくことが提案されている[57]。

ワークショップの研究発表からは、STPA-sec[58]を使った分析から改善策を導き出せなかった事例も出てきている。システムの肥大化、複数のハードウェアの制御、ネットワーク化など様々な対応を日々迫られる航空業界では、航空機のメンテナンス時に整備員がソフトウェアを更新する Field Loadable Software（FLS）と呼ばれるシステムを使用しており、MIT の研究室では、ソフトウェア更新により発生する事故を回避する目的で STPA ベースのハザード分析を行っている。この分析からは、航空機メーカーから適切なソフトウェアがネットワークを通して送られてきた場合でも、サイバー攻撃などによりソフトウェアが改ざんされたり、整備員が誤ったソフトウェアをインストールしたりするというリスクが発覚している。しかしながら、整備員や航空機のパイロットがどのようにしてソフトウェアを確認するかという問題や、整備員がソフトウェアに不具合を発見しながらも放置した場合にどのような対応が必要になるかなど、STPA を使ったハザード分析から抜本的な改善策へは至っておらず、今後の課題となっている[59]。**図表 16** は Field Loadable Software のイメージ図となっており、左の図は更新用ソフトウェアのやり取りを示しており、右の図は飛行機に搭載された Field Loadable Software である。

図表 16：Field Loadable Software のイメージ図



出典：MIT を基に作成[60]

[57] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STPA-Tutotrial.pdf
[58] STPA をサイバーセキュリティの対策へ応用する手法。
[59] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Helfer-aviation-software-presentation.pdf
[60] http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Helfer-aviation-software-presentation.pdf

6　終わりに

昨年に引き続き STAMP をテーマにとりあげたが、一年前に比べて、さらに実用化が進み、各方面でその有用性が実証されている。また、5 章で取り上げたように、ハザード分析して設計変更した結果新たに生じる課題を、ハザード分析を反復することで解消させる方策など、より確実なハザード分析が行えるような取り組みも進み、実用面でさらに精度が高まっていると言える。
他方、同じく 5 章で取り上げたように、実際の場面では、まだ考慮しなければならない要因が出てくるなど、新たな課題も判明してきた。しかし、これは実用化が一層進んだ結果とも言える。今後、より実用化を進めることで、STAMP 自身がさらに改良され、高度なシステムにおける事故の減少に一層貢献していくことが期待される。
今年の STAMP ワークショップも、昨年に引き続き世界各国から多くの参加者が集まり、活発な議論がなされ、STAMP に対する注目・期待の高さを改めて感じた。我が国でも、今後 STAMP がさらに普及し、高度なシステムが支える社会がさらに発展することを期待したい。

（2015 年 6 月 18 日に東京で、IPA 主催の SEC 特別セミナー「システムベースのエンジニアリング最新動向（複雑化するシステムの安全性とセキュリティを確保するためにすべきこと！）」を開催し、マサチューセッツ工科大学のナンシー・レブソン教授による STAMP の最新動向に関する講演などを行う予定です。詳細の案内・お申込みは以下の URL をご覧ください。
（http://sec.ipa.go.jp/seminar/20150618.html））