システムの相互作用に着目したこれからの安全（STAMP）

金子朋子
IPA
中沢 潔
JETRO/IPA New York

1. サマリー

STAMP（Systems-Theoretic Accident Model and Processes）[1]は、2012 年にマサチューセッツ工科大学（MIT）教授のナンシー・レブソン（Nancy Leveson）氏が提唱した安全性解析手法である。その背景には、IoT の普及などによりシステムが複雑化する中で「各構成要素のアクシデント対策だけではシステム全体のアクシデント防止には不十分である」という状況がある。例えば、かつて、空中では飛行機に逆推進させないよう制御するソフトウェアが、雨に濡れた地上でのハイドロプレーニング現象によって着陸したことを理解できないために作動せず、事故が発生したことがある。これはソフトウェアのデザインの問題であり、機体の各機器に故障があったわけではない。この事象の解決には従来のようにシステムの構成要素である各機器のハードウェア的なアクシデント対策をするだけでなく、ソフトウェアを含めて相互作用を検討する必要がある。STAMP はこのように現在の複雑なシステムの安全を保つため、ハードウェアとソフトウェア、さらに人や組織との関係まで含めた分析を行うものである(図表 1、図表 2)。また、安全性のみならず、サイバーセキュリティやプライバシー等の特性を統合的に分析できることも大きな特徴である。

STAMP が提唱されて以来、その研究者や実践者が一堂に会する MIT STAMP Workshop が毎年開催されている。第 7 回目を迎えた MIT STAMP Workshop 2018（2018 年 3 月 26 日～29 日）は 32 か国から 325 名の参加を得た。事例発表の対象業界は、防衛、自動車、航空、医療、ライフライン、海洋、鉄道、宇宙と多岐に渡る。日本企業の参加者は自動車関係が最多である。特に、大規模組織への適用効果や標準化について以下のプレゼン等が行われた[2]。

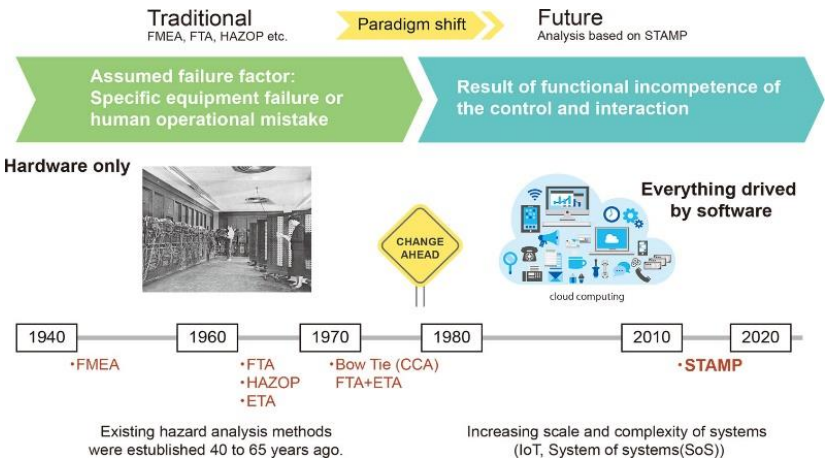
- Boeing 社
  広く多様なシステムズエンジニアリングに STAMP を適用した結果、安全だけでなく、品質、サイバーセキュリティという複数の特性に適用できることが明らかになり、システムのハードウェア、ソフトウェア、人間と環境のインターフェースと相互作用を分析できた。さらに製品のライフサイクルのすべてのフェーズに適用可能であり、従来の方法よりも効率的で効果的である。例えば、工場ロボット解析においては、システム設計上の欠陥を生む安全でないシステム条件を、従来に比べ 8．5 倍抽出でき（2 件から 17 件）、"なぜ"事故が発生しているのかの答えが得られ、38 のリスク要因を洗い出し、事前対処できた。

---

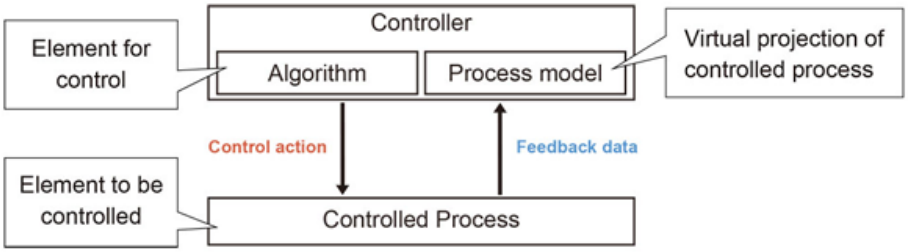
[1] STAMP の概要及び過去の報告は以下を参照されたい。
https://www.ipa.go.jp/sec/our_activities/stamp.html
http://monoist.atmarkit.co.jp/mn/articles/1803/09/news013.html
http://jif.org/column/pdf2015/201505.pdf
http://jif.org/column/pdf2014/201406.pdf
http://jif.org/column/pdf2014/201406.pdf

[2] http://psas.scripts.mit.edu/home/

- GM 社
  ISO26262（自動車の電気電子システムの機能安全に関する規格）[3]が HMI（Human Machine Interface）の観点から、人間の行動の評価に十分には対処していないため、同社の正式な安全プロセスの一部として STAMP/STPA[4]を採り入れた。また、SAE（米国自動車技術会）機能安全委員会の下におかれた SAE・STPA 推奨事項の実践タスクフォースが、ISO26262 も含め、STPA の実装と使用に関して自動車業界全体に普及活動をしている。



図表 1　出典：IPA



図表 2　出典：MIT

またワークショップに先立って、本年（2018 年）3 月に MIT から STPA ハンドブックが公開された。同ハンドブック第 3 章には、システムエンジニアリングと STPA の関係が新たに明示された。従来コンセプト段階でのリスク分析を中心に利用されてきた STPA がライフサイクルを通じて利用できることが明示された意義は大きい。

IPA は、2017 年 11 月に「第 2 回 STAMP ワークショップ in Japan」を開催し[5]、また 2018 年 3 月には、STAMP の導入を容易にするモデリングツール「STAMP Workbench」を無償公開している[6]（MIT STAMP Workshop 2018 においてレブソン教授から参加者にも紹介）。日本のワークショップは本年（2018 年）も開催を予定している。

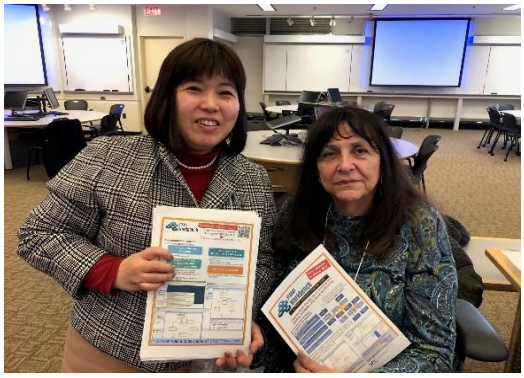
---

[3] http://www.jari.or.jp/tabid/112/Default.aspx

[4] System Theoretic Process Analysis：STAMP 理論に基づく、相互作用する機能単位でリスクを考える安全性分析手法。

[5] https://www.ipa.go.jp/sec/events/20171127.html
https://www.ipa.go.jp/english/sec/complex_systems/stamp_workshop.html

[6] https://www.ipa.go.jp/sec/tools/stamp_workbench.html#outline



図表 3　MIT　Nancy　Leveson 教授と筆者（金子）

2. MIT STAMP Workshop 2018

ここではワークショップの内容、注目すべき発表、産業別の動向などについて具体的に伝えたい。

(1)ワークショップ概要

本ワークショップは、初日 1 日のチュートリアルと 3 日間のプレゼンテーションで構成される。このうちチュートリアルについては、基本編として STAMP・STPA・CAST[7]のイントロダクション、および応用編として STPA・CAST のファシリテーション、主要指標の作成と使用、サイバーセキュリティにおける STPA をテーマに開催された。

図表 4　チュートリアル内容一覧（出典：MIT）を基に作成

ビギナー用	経験者用
STAMP イントロダクションと STPA と CAST の概要（Prof.　Leveson）	STPA・CAST のファシリテーション（Dr.Thomas）
STPA　イントロダクション（Dr.Thomas）	主要指標の作成と使用（Prof.Leveson）
STPA 実務 CAST イントロダクション、事例（Prof.Leveson）	サイバーセキュリティにおける STPA（Dr.Young）

イントロダクションは毎年実施され、少しずつ改訂されており、具体例を用いて演習的な要素を取り入れている。

同ワークショップは、当初の研究者中心の国際会議から、企業で適用され、効果を発表する場に成長してきている。発表を分類すると、下表のようになる。昨年 1 件だった医療とライフラインがそれぞれ 5 件、4 件に増え、当該分野への適用が広がっている。

図表 5　発表内容一覧（出典：MIT）を基に作成

タイプ	対象・業界	
方式（手順）の提案ツール	コンパイラ技術と STPA の組み合わせ	
	STPA のサポートツール	
	ソフトウェア検証 BDD と STPA の組み合わせ	
STPA の適用	空軍の調達技術要件開発	防衛
	自動運転システムでのヒューマンエラー軽減	自動車

[7] Causal Analysis using System Theory：STAMP 事故モデルの考えに基づいた不具合分析手法。

	航空機コントロール事故の低減	航空
	医療機器におけるユーザインタフェースソフトウェア解析の改善	医療
	安全な処方プロセス設計	医療
	放射線治療における STPA の応用: 予備的研究	医療
	放射線治療における STPA の経験	医療
	自動運転システムのためのプロセスモデルへの行動能力の構築	自動車
	自動運転車のテストシナリオ	自動車
	水力発電の STPA アプリケーション	ライフライン
	航空安全管理システムの自己評価のための AVAC-SMS 測定基準	航空
	水供給システムにおける技術仕様と主要安全指標	ライフライン
	海底操作への STPA 適用	海洋
CAST と STAMP/STPA の考えの適用	航空機事故の再比較分析	航空
CAST の適用	フランス国営航空機をめぐる事故やインシデントへの安全調査	航空
	米国貨物鉄道での信号オーバーラン阻止のためのアプリケーション	鉄道
	妊娠時の薬剤服用	医療
	国際宇宙ステーション EVA23 スーツへの水侵入事故	宇宙
	アシアナ航空 214 便事故への適用	航空
	シドニー水危機のシステム分析	ライフライン
STPA-Sec セーフティ & セキュリティ	空中給油機のケーススタディ	航空
	核セキュリティ文化の評価における STPA 利用	ライフライン
	L4 自動運転への STAMP Safety and Security 分析適用	自動車

STPA-Sec ではサイバーセキュリティにおけるエンジニアリングとして STPA からセキュリティ拡張した部分の特徴が説明された。本チュートリアルに今年は多くの日本人が参加しており、日本における STPA セキュリティへの関心の高まりが感じられた。パネルディスカッションでは標準化推進と大規模組織への適用結果のプレゼンがなされた。また Boeing 社、GM 社、Embraer 社、Fatima Group 社が STPA、CAST を幅広く適用してきたことにより、自社の業務に対して有効性があったことが発表された。

また、航空、自動車、ライフライン、医療など、参加者の産業別のランチタイムミーティング（Birds of a Feather Session）が開催された。自動車産業のミーティングでは、GM 社の技術フェローを中心に自動運転の課題、ISO26262 に STPA はどう対処するか、STPA は小さな部品、コンポーネントをどう扱うか、SAE の STPA 推薦実施事項、SOTIF（Safety Of The Intended Functionality）問題への対処などが話し合われた。なお、MIT のコンソーシアムメンバーによる自動車のセーフティに関してのミーティングも別途、開催された。

（2）Boeing 社事例と航空業界の標準化

Boeing 社のディレクターからは同社における STAMP を適用した広く多様なシステムズエンジニアリングの成功事例とその理由が紹介された。詳細は以下の通り。

＜主な利点＞

・セーフティと同様に品質、スケジュール、サイバーセキュリティ上の損失を防げる。
・既存のモデリングと解析ツールを補完するために、どんなシステムにも適用可能。
・システムのハードウェア、ソフトウェア、人間と環境間のインターフェースと相互作用を分析可能。
・メソッドを製品のライフサイクルのすべてのフェーズに適用可能。

・従来の方法よりも効率的で効果的であることを証明。
・ニーズに合わせて規模変更や構成要素の組み合わせが可能。

＜STAMP を使用したシステムエンジニアリング＞

・障害につながる仮定を上流工程で見つけ、顧客とのさらなる議論で情報の不完全な点を発見可能。
・既存システム分析や初期のアーキテクチャ、予備的設計に対し品質、効率性、セキュリティ、安全性の要件を提供可能。
・上流からの設計上の欠陥を下流工程へ持ち込むのを防ぐため、コスト負担を大幅に削減。
・システムの脆弱性に関する深い洞察を与えるため、サイバーセキュリティに有用。

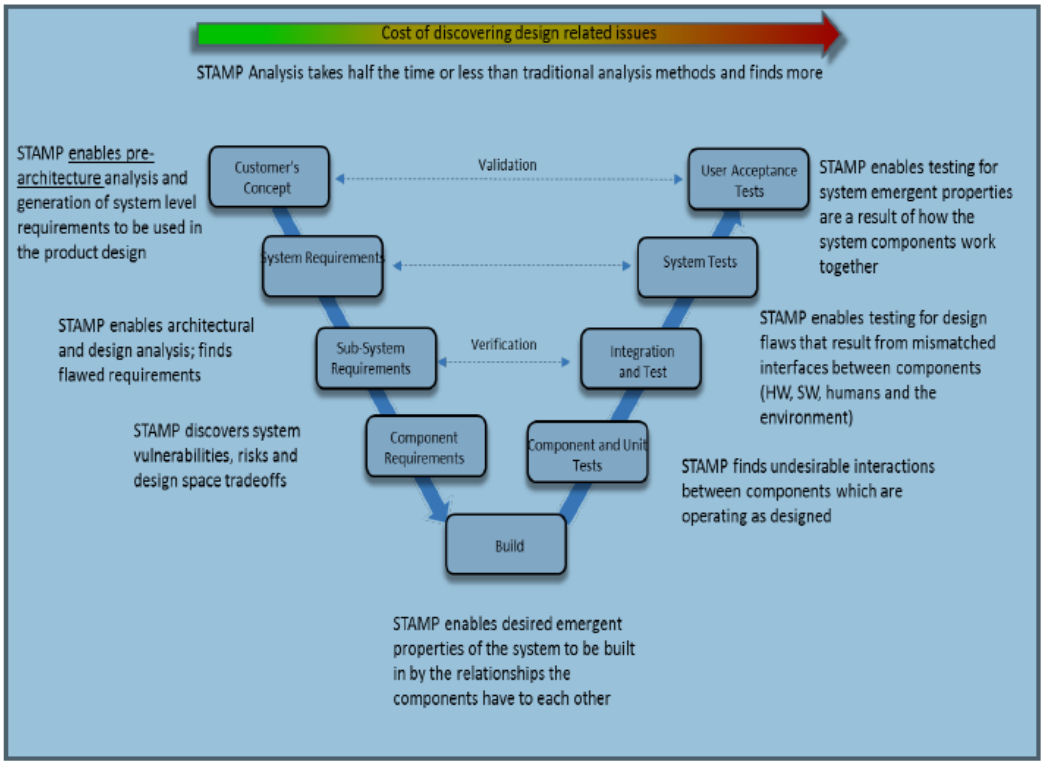
＜サクセスストーリー＞

・コンセプト開発という早期段階で潜在的な設計上の以下の欠陥を識別。国防総省で急速に支持を得た。

- 54 パイロット/フライトマネージメント
- 84 アビオニクスシステム
- 23 フライトコントロールコンピューティングシステム（FCC）の安全でないアクション
- 34 飛行制御作動

産業用ロボット解析においては、システムに設計上の欠陥を生む安全でないシステム条件を、2 件から 17 件と、従来に比べ 8. 5 倍抽出できた。さらに 38 因果シナリオを作成し、"なぜ"事故が発生しているのかの答えが得られ、38 の潜在的な制御とシステム設計の変更につながった。他の 3 つの成功事例も定量的に効果が示された。

結論として、STAMP は非常に複雑なシステムを簡素なモデルで記述し、分析する機能を備えている。STAMP/STPA は安全だけでなく、サイバーセキュリティ、品質等の複数の特性に適用できる。。ハードウェア、ソフトウェア、ヒューマンインタラクションを伴う複雑なシステムとの分析に最大の利点をもつ。

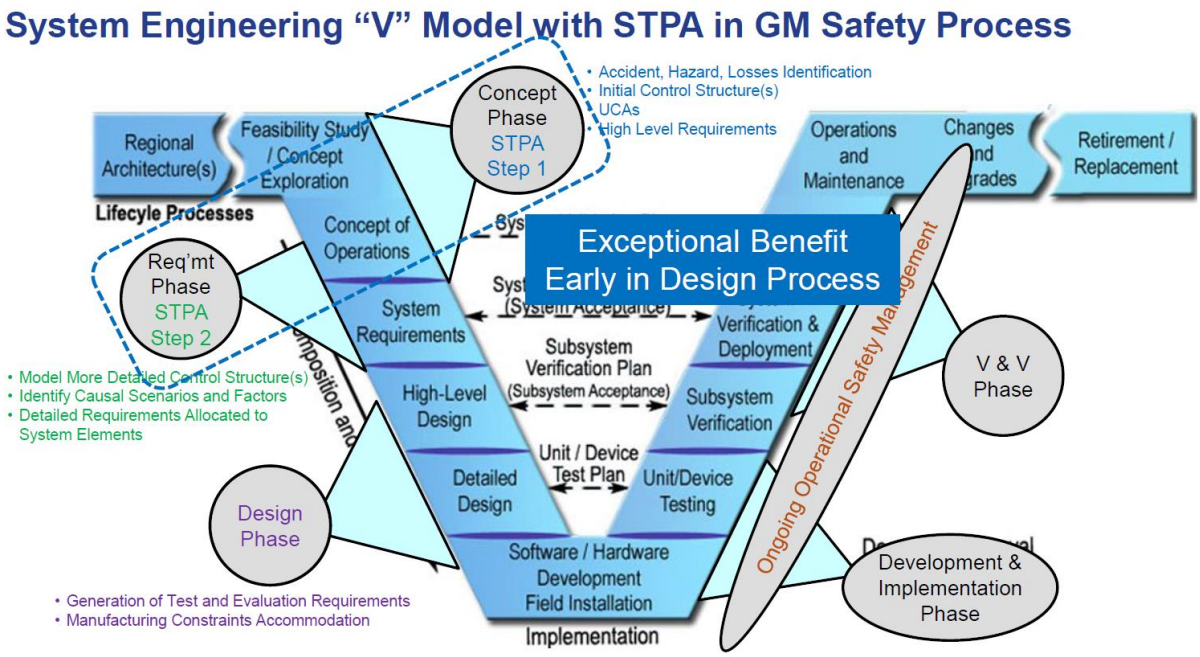


また、Boeing 社のアソシエイト技術フェローは、航空機標準における STPA の役割を紹介。SAE S-18 委員会は ARP 4761（安全性評価プロセスガイドラインとメソッド）、ARP 4754/ED-79（航空機・システム開発プロセス）において、民間航空機の開発と安全性評価への STPA 適用を推進。具体的には STPA が ARP4754 および ARP4761 フレームワークにどのように関連しているかを示し、STPA の長所と限界について、航空宇宙産業に基本的な理解を促進し、認証に用いることを検討している。

(3)GM社事例と自動車業界の標準化

GM 社におけるシステム安全プロセスへの STPA の統合状況が紹介された。ISO26262 が HMI（Human Machine Interface）の観点から、人間の行動の評価に十分には対処していないため、（同社の）正式な安全プロセスの一部として STAMP/STPA を採り入れた。STPA で生成された要件は、安全文書に取り込まれ、正式な要件文書に割り当てられている。STPA による分析結果は安全制約として反映される。

図表 6 STPA-Sec テーラリング方式評価（出典：MIT）



図表 7　GM 社のセーフティプロセス（出典：MIT）

SAE（米国自動車技術会）機能安全委員会の下におかれた SAE・STPA 推奨事項の実践タスクフォースが、ISO26262 も含めて、STPA の実装と使用に関して自動車業界全体に普及活動をしている。

活動の特徴は以下の通り。

＜スコープ＞

自動車車両の安全に焦点を当てた安全評価プロセスにおいて、STPA の教材と推奨事項を提供。

＜目的＞

この活動は自動車の制御、自動車の HMI、および自律走行等における STPA の実装と使用に関して自動車業界全体への説明を目的としている。

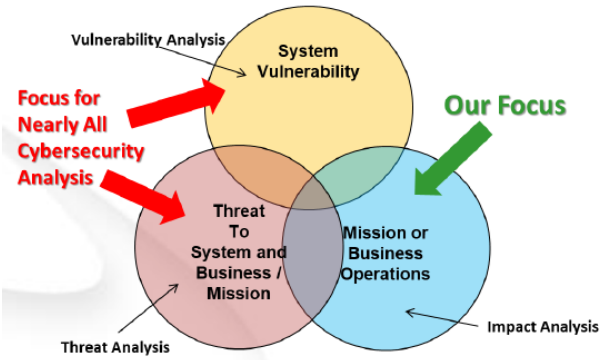
＜関連事項＞

SAE 機能安全委員会、ISO26262、および ISO SOTIF PAS initiatives に STPA を調和させる活動である。

（4）STPA セキュリティ（STPA-Sec）のテーラリング（標準のカスタマイズ）事例

AFIT(Air Force Institute of Technology:空軍技術研究所)による STPA-Sec の空中給油機のケーススタディでは、以下の点が示された。

・どのように STPA-Sec がセキュリティ要求と設計基準を満たすようにテーラリングできるのか？
・STPA-Sec は USAF（United States Armed Forces:米国空軍）の相互戦闘システムにどのように適用できるのか？
・STPA-Sec のユーティリティと容易性を高めるのにどんな推奨事項があるのか？

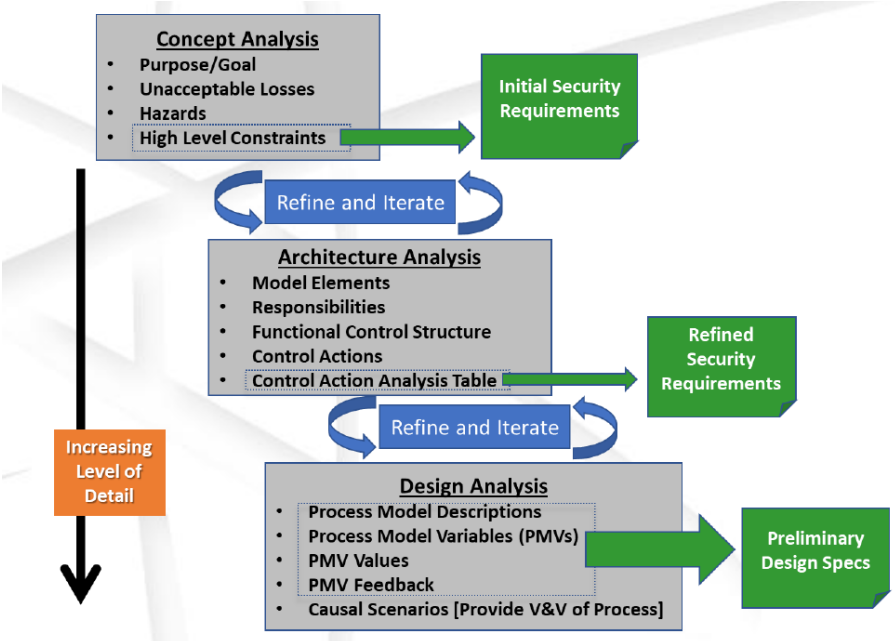


図表 8　脆弱性分析、脅威分析、問題分析（出典：MIT）

本事例は脆弱性分析、脅威分析、問題分析の中でミッションやビジネス運用における問題分析に焦点をおいている。（図表 8）

本事例では下図のように STPA-Sec のテーラリング方式が初めて示された。この方式は以下の手順である。

・概念分析で目的／ゴール、受け入れられない損失、ハザードを求め、ハイレベルの制約を初期セキュリティ要求として抽出する。
・次にアーキテクチャ分析をし、モデル要素、責任、機能コントロールストラクチャー、コントロールアクション分析表を作成して、洗練されたセキュリティ要求を求める。
・さらにデザイン分析でプロセスモデル記述、プロセスモデル変数、PMV バリュー、PMV フィードバックを設計仕様とし、要因シナシオを作成、V&V プロセスを提供する。
・概念分析からアーキテクチャ分析、デザイン分析へレベルの詳細化を行い、改善を繰り返す。



図表 9　STPA-Sec テーラリング（出典：MIT）

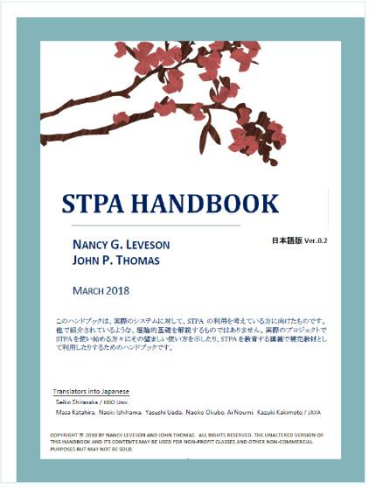
このテーラリング方式の適用の目的、難易度、ドメイン知識要求度、STPA 知識要求度、STPA の教育教材の必要性、期間、ステップ数が以下の表で示された。

	Concept Analysis	Architectural Analysis	Design Analysis
Purpose	Determine Security Requirements	Determine Design-To Criteria	Determine Build-To Criteria
Difficulty	Easy	Moderate	Moderate-High
Level of Domain Expertise Req'd	Novice	Advanced	Expert
Level of STPA Expertise Req'd	Low	High	Moderate
Amount of STPA instructional materials available	Numerous	Some	Few
Duration	Hours	Days	Weeks
Number of Steps	4 Steps	5 Steps	5 Steps

図表 10　STPA-Sec テーラリング方式評価（出典：MIT）

3.　STPA ハンドブック

本年 3 月に公開された STPA ハンドブックは理論的基礎を解説するものではなく、プロジェクトでの利用方法の参考とする補完教材である。MIT の HP には英語版と共に日本語版も掲載されている。
ここでは同ハンドブック第 3 章で新たに提示された、STPA をシステムエンジニアリングに関わる様々なフェーズや活動へ適用する方法を紹介する。

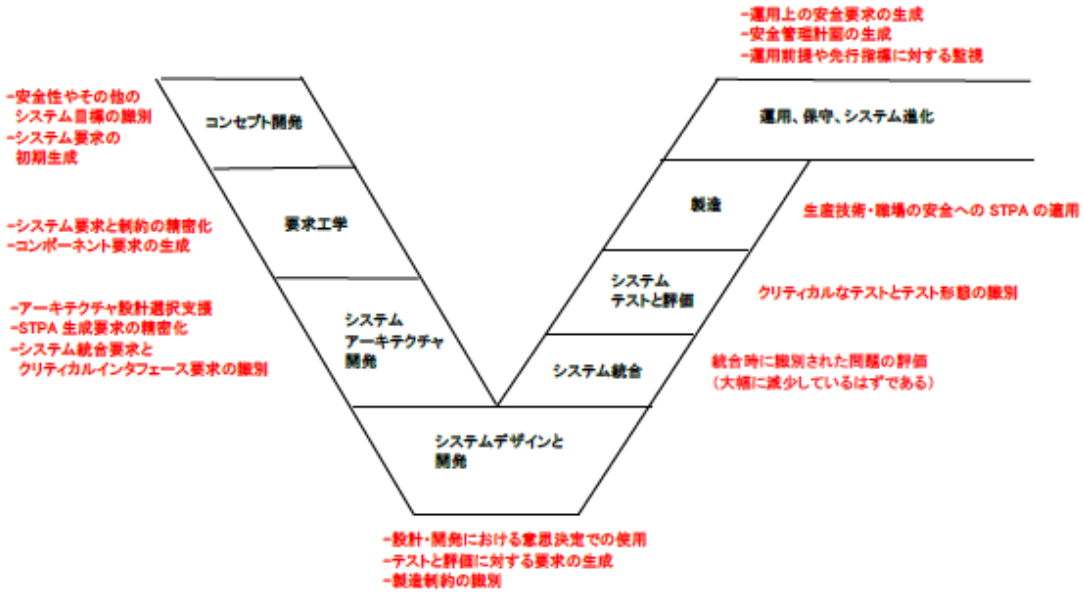


図表 11　STPA ハンドブック（出典：MIT）

図表 12 は標準的なシステムエンジニアリングプロセスの V 字モデル（またはウォーターフォールモデル）を簡略化したものである（フィードバックループは簡素化のために省略している）。本図は、STPA を標準的なシステムエンジニアリングプロセスにどのように統合するかを示し、その中で STPA の役割候補を赤字で示している。

様々な V 字モデルや他の開発プロセスモデルがあるかもしれないが、この標準的な V 字モデルから置きかえて解釈することは難しいことではない。ただし最上流（V 字 左上部の 2 つのプロセス）は重要であり、これが省略されているようなプロセスでセーフティクリティカルなシステムを構築すべきではない。

システム全体のエンジニアリングプロセスにシステム安全性解析を密に統合できれば、大きな効果をもたらすだけでなく、安全に関するエンジニアリングコストは大幅に削減できる。また手戻りが減り、コスト低減や期間短縮も見込まれる。

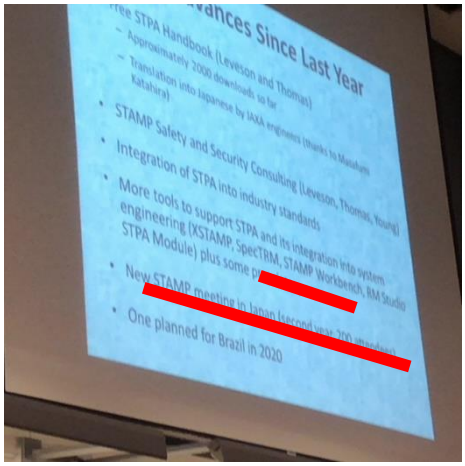


図表 12　システムエンジニアリングプロセスへの STPA の統合（出典：MIT）

4. IPA の取り組み

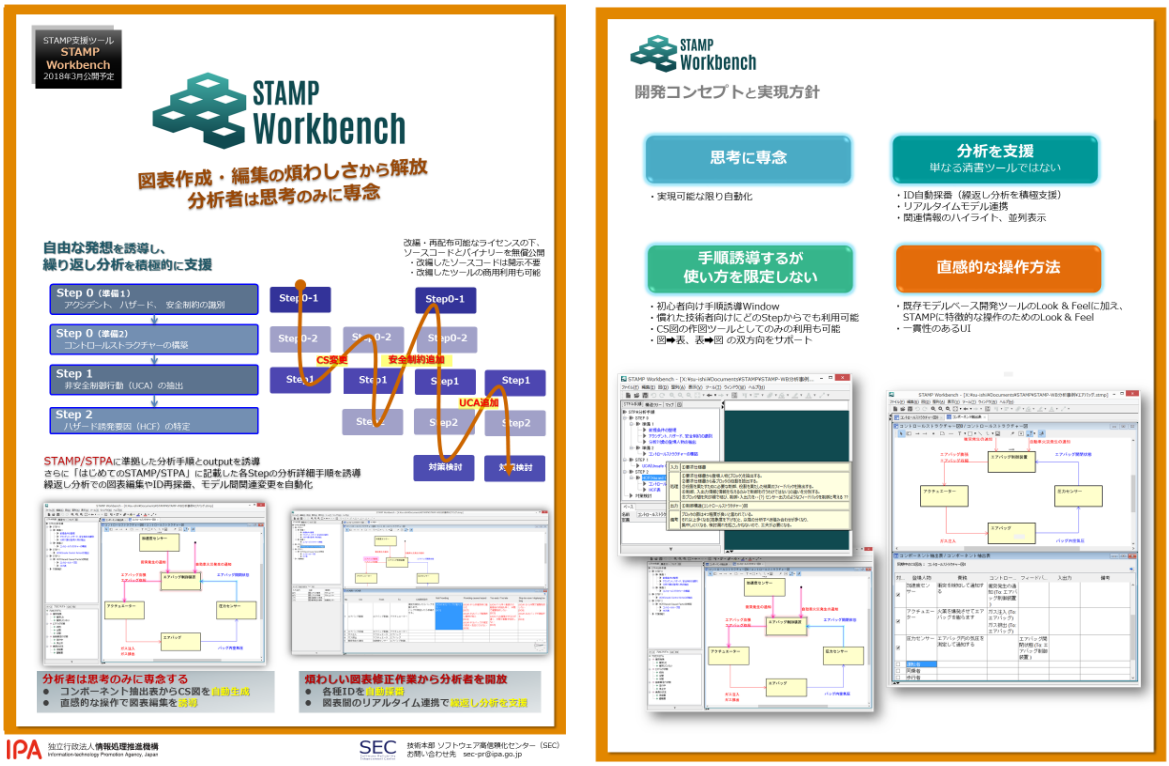
本ワークショップの Welcome スピーチでレブソン教授は、日本の IPA の取組みとして、STAMP Workbench や日本で昨年 11 月に IPA が開催した第 2 回 STAMP ワークショップを紹介した。

海外には、XSTAMPP などいくつかの STAMP 支援ツールがあるが、いずれも STAMP 研究者が STAMP 研究者のために開発したものであって、
産業界で実際のシステムの安全性解析を行う技術者による分析を支援するツールは他にはなかったため関心を集めた。



図表 13　Welcome　Speech 資料

この STAMP Workbench は英語版マニュアル、サンプルファイルが用意され、IPA の英語サイトよりダウンロード可能である。
https://www.ipa.go.jp/sec/reports/20180330.html



図表 14　STAMP　Workbench　ちらし（出典：IPA）

第 2 回 STAMP ワークショップ　in Japan は、2017 年 11 月 27 日から 3 日間にわたって開催された[8]。本年も STAMP ワークショップ　in Japan は IPA により開催される予定であり、多彩な発表を期待したい。

※ 本レポートの内容に関して、その有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。