第 2 回 STAMP ワークショップ in Japan 実施報告

第 2 回 STAMP ワークショップ in Japan
実行委員会

●開催概要

1 年前に福岡市で開催された第 1 回に引き続いて、第 2 回 STAMP ワークショップ in Japan は、場所を東京都にある慶応義塾大学三田キャンパスに移し、2017 年 11 月 27 日から 3 日間にわたって開催された。

4 カ国から延べ 181 名(前回は 117 名)の参加者が集まり、初日に米国 MIT からの基調講演/チュートリアル、欧州 STAMP ワークショップ（ESW）からの招待講演が順に行われ、その後、一般講演として産業界から 13 件、学術界から 11 件、合計 24 件(前回は 16 件)の発表が行われた。あわせて、ポスター展示が 2 件(前回は 0 件)あり、今年度に開発中の STAMP 支援ツールである「STAMP Workbench」が紹介され、期間中、デモ展示された。

概略日程は次のとおり:

2017 年 11 月 27 日(月)

9:35-9:45	実行委員長挨拶
9:45-11:45	基調講演/チュートリアル
12:45-14:15	基調講演/チュートリアル
14:30-15:30	招待講演
15:40-17:00	Overseas and Tools Session(3 件)
17:00-18:00	挨拶、ツールのデモ展示

2017 年 11 月 28 日(火)

9:00-10:50	ショートセッション(4 件)、標準セッション(1 件)
11:00-12:30	標準セッション(3 件)
13:30-16:00	標準セッション(5 件)
16:10-17:40	標準セッション(3 件)

2017 年 11 月 29 日(水)

9:00-11:30	標準セッション(5 件)
11:30-12:00	クロージング

なお、STAMP ワークショップに関する Web サイトを IPA/SEC が運営しており、その URL は次のとおり:
(日本語) https://www.ipa.go.jp/sec/our_activities/stamp.html
(英語)
https://www.ipa.go.jp/english/sec/complex_systems/stamp_workshop.html

●発表概要

今回の講演資料は、そのほとんどが IPA/SEC Web サイトに掲載されている (https://www.ipa.go.jp/sec/events/20171127.html)。この節では、概要のみを記載する。

(1)チュートリアル

前回同様、MIT の Dr. John Thomas が担当し、3 件のチュートリアルを行った。その概要は次のとおり:

T1 : STAMP and STPA Introduction

多くの事例を用いて、STAMP の必要性と特徴を説明し、STPA 分析の概要を紹介。

T2 : STPA Exercise

米国 DoD(Department of Defense) Access control barrier の題材を用いて、STPA 手順を演習を交えて順に詳細解説。

T3 : Advanced STPA Topics

前回同様に、APA (Automated Parking Assist : 自動駐車支援機能) に対する STPA 分析結果を解説。

(2)招待講演

European STAMP Workshop Board から Dr. Nektarios Karanikas (アムステルダム大学) が来日し、次の招待講演を行った:

G1 : Situations of STAMP in Europe

欧州における STAMP の実情に関して、コミュニティ、ワークショップ、推進委員会、教育と

研究などについて紹介。

(3)産業界からの一般講演

I1：STAMP/STPA の自動車向けの活用ガイド-JASPAR 機能安全 WG 活動成果より-(JASPAR)

仮想的な電動パーキングブレーキシステムに STPA を適用し、ISO 26262 との差分分析を行い、開発現場向けの活用ガイドを作成した。

I2：システムモデルを用いた STAMP/STPA 試行の事例紹介(日立産業制御ソリューションズ)

仮想的なドライバ異常時安全停車システムを題材として、開発初期に作成される、抽象度の高い SysML モデルを活用して STPA 分析を実施した。

I3：国際安全規格における STAMP/STPA 適用可能性の考察(東芝)

STPA が国際安全規格において、従来の安全分析手法との違いを踏まえて、どの開発工程に適するかを、規格、従来手法、STPA 適用事例などを調べて考察した。

I4：自動運転系の安全・セキュリティ解析のための自動化ヒューマンファクタに基づく STPA ガイドワードの提案(日立製作所)

自動化システムの監視制御系において、ヒューマンファクタに基づくハザード誘発要因を識別するためのガイドワードを提案し、自動運転系などに適用を試み、その有用性を確認した。

I5：STAMP による閉電路制御式踏切制御システムの安全性評価(京三製作所)

従来方式と新方式による踏切制御システムに STAMP/STPA を適用し、STAMP による安全性評価の有効性を確認した。

I6：STAMP/STPA の鉄道信号システムへの応用と拡張(東日本旅客鉄道)

STAMP/STPA を信頼性についても拡張し、鉄道信号システムにおけるこれまでの事故や不具合などを評価した。

I7：STAMP/STPA を用いた踏切障害物検知システムの安全性分析(東日本旅客鉄

道)

踏切障害物検知システムに STAMP/STPA を適用し、ハザード誘発要因を識別するとともに、設計上の安全制約を抽出した。

I8：STAMP/STPA による踏切制御システムの安全性要求分析(東日本旅客鉄道)

新たに試作した構内踏切制御論理に STAMP/STPA を適用して安全解析を実施し、安全要求事項の抽出を試みた。

I9：意図・要求記述レベルの STAMP/STPA 手法(JASA)

仮想的な電動アシスト自転車開発を題材とし、開発に関する意図と要求の記述をもとに STPA 分析を行い、その結果、意図の実現に適する推奨策を導出した。

I10：Extending STPA をベースとしたプロセスモデル抽出の工夫(日本ユニシス)

Extending STPA において 6W3H の視点からコンテキストを抽出する工夫を提起し、自動運転制御システムを題材にそれを試行した。

I11：STAMP/STPA を用いた Cyber-Physical Systems の検証(日本ユニシス)

複雑になるコントロールストラクチャを整理する方法と，そのコントロールループの安全な状態をモデル検査により検証する手法を提起し、例題として Vehicle-to-Device (V2D) システムを利用した車の交通制御システムに適用した。

I12：STAMP/STPA を用いたリスクマネジメントフレームワークの提案(電通国際情報サービス)

既存のリスク抽出・管理方法に STAMP/STPA を用いることで、メカ観点でのリスクだけでなく制御観点でのハザードを共に抽出・管理できることがわかり、技術的なリスク管理だけでなく、開発日程面でのリスク管理もできるフレームワークを構築した。

I13：STAMP を STAMP してみた！(オムロンオートモーティブエレクトロニクス)

観光地や駅などにおかれている記念スタンプを題材に、STPA の基本手順を辿り、課題や利点などを考察した。

(4)学術界からの一般講演

A1 : Integration of Security into CAST (Zurich University of Applied Sciences)

セキュリティ侵害を分析する手法を CAST プロセスに統合させ、代表的なセキュリティ事故に適用してその有用性を確認した。

A2：STAMP ベース・ハザード分析ツールの紹介(仙台高等専門学校)

STAMP/STPA 分析を支援するツールとしては、専門ツールや流用できる関連ツール等があり、それらの特徴を調べた。

A3：IPA が提供する STAMP 支援ツール i-STAMP(開発コード) (IPA/SEC)

STAMP/STPA 分析作業を支援して、思考に専念できるように、IPA はツールを年度末リリースを目標に開発している。

A4：プロジェクト管理における動機付けに着目した STAMP/STPA の適用(長崎県立大学)

プロジェクト管理の制御構造を STAMP によってモデル化し，STPA 分析によって制御構造の適正化や運用指針の策定を行うアプローチを考察した。

A5：Freedom from interference に着目した STAMP/STPA の適用(長崎県立大学)

AADL(Architecture Analysis & Design Language)を使用するシステムアーキテクチャの記述や分析に STAMP/STPA を適用した。

A6：STAMP/STPA 事例の振り返りと GSN を用いた STPA プロセスの説明支援(日本大学)

STAMP/STPA 手順を行う上での課題及び工夫を抽出し、実施する際に重要なポイントをまとめ、 GSN(Goal Structuring Notation)により表記した。

A7：STAMP/STPA を用いた自動運転システムのリスク分析-高速道路での合流-(愛知工業大学)

自動運転システムと運転者の連携に着目して，特に危険が多いと考えられる自動運転中の高速道路の合流に STAMP/STPA を適用した。

A8：STAMP/STPA による多目的バッチプラントのリスク解析(名古屋工業大学)

マルチパーパス/マルチバッチといったフレキシブルな運用を行う化学プラントに対して、原料や洗浄液のコンタミネーションなどに注目して STAMP/STPA を適用した。

A9：電動アシスト自転車を対象としたハザード分析/STAMP・STPA と数値シミュレーションの特徴比較(会津大学)

電動アシスト自転車という人間・機械の協調制御システムを題材に、STAMP/STPA によってどのようなハザード要因が分析可能かを検討し、 SimuLink に代表される数値分析によるハザード分析との比較により、STAMP/STPA の有用性を示した。

A10：コントロールストラクチャの状態遷移仕様とガイドワードを用いたシミュレーションによる STAMP/STPA の非安全コントロールアクションの識別方式の提案(大阪工業大学)

コントローラ及び被制御プロセスの仕様を状態遷移仕様で表し、ハザードとなる状態への到達可能性をガイドワードに則ってシミュレートすることで、UCA を半自動的に識別する方式を考察した。

A11：IoT/深層学習利用における STAMP と HAZOP についての研究(名古屋市工業研究所)

STAMP に注目して、HAZOP や FRAM 等の他手法との相違を整理した。

●傾向と課題

一般講演の傾向を明らかにするために、発表内容に応じて次の 4 種別で分類してみた:

試行事例：STAMP の適用可能性を評価するために、試験的に適用を
　　試みた事例の紹介
活用事例：現在使用している、開発している、又は研究している製品や
　　システムなどに STAMP を適用した結果の紹介
手法解説：仮想的な題材をもとに、STAMP を適用する手順、適用するときの
　　工夫や考慮事項などを解説するもの
手法改善：標準的な STAMP 関連手法の拡張や詳細化を研究し、

その改善を提案するもの

分類の結果を表 1 に示す。この表から次に列記する傾向が読取れる:

- 学術界からの発表は、手法解説に偏っているが、産業界からはどの種別にもほぼ同じ件数の発表がある。
- 試行事例の件数は産業界と学術界でほぼ同じである。産業界は、開発済みの制御システムを題材としているが、学術界は、制御システム以外にも目を向けている。
- 活用事例と手法改善は、産業界から多く発表されているが、開発中又は今後のシステムに適用してみようという産業界の意欲が感じられる。
- 産業界から手法改善が多かったのは、適用プロセスの標準化を目指して、手法の定型化を求めていることによると考えられる。

表 1　一般講演の分類結果

	産業界からの一般講演	学術界からの一般講演
試行事例	I5　I6　I7	A4　A5　A7　A8
活用事例	I8　I9　I12	
手法解説	I1　I3　I13	A1　A2　A3　A6　A9 A10　A11
手法改善	I2　I4　I10　I11	

最後に、今回の開催を振り返り、次回以降に改善すべき事項を指摘すると、次に列記するとおり:

- 3 日間という会期については、短くするか、あるいは、聞く前に発表の種別がわかり、選択的に聴講できる等の工夫が欲しい。
- 応募時の工夫として、STAMP 適用時の課題である、プロセス変数の抽出、コンテキストの識別、制御構造図の作成等に関する解決策を募集することが考えられる。
- チュートリアルについては、同じように短くするか、あるいは、ハンズオン的なものや議論する場の提供などを検討したい。
- チュートリアルを通訳無しの英語で実施したが、参加者が少なかったことを考えると、再考の余地がある。
- 発表時間は、標準セッションで 30 分だが、説明時間を減らし、Q&A の時間を多く確保するように運営したい。

- Q&A については、質問者が特定の人に偏らないように、誰でも気楽に質問できる場作りが必要である。
- 予約が満員に達して予約できない人が出たが、当日の不参加者も多く、対策が必要である。

これらの改善事項に対処し、今後、試験的な試行事例から一歩進んで、STAMP 適用時の課題の解決策、関連手法の改良、深化等を提案する発表が増え、実際の開発案件に活用されていくことを期待してやまない。