G-12

# システム思考に基づくリスク分析手法 STAMP の試行および web ベース STAMP ツールの設計と開発に向けて

# A Trial of STAMP: A Systematic Risk Analysis Method and Toward Design and Development of Web-based STAMP Tool

○阿部惇朗 [1], 古川優也 [1], 松野裕 [2]
*Junro Abe[1], Yuya Furukawa[1], Yutaka Matsuno[2]

Abstract: Systems become huge and complex, and causes of failures includes not only causes inside a system component, but also causes by interaction among system components and humans. Recently, STAMP (Systems-Theoretic Accident Model and Process) has been proposed for analyzing failures by interaction among system components and humans. However, currently STAMP has not been well prevailed. This is because that basic usage of STAMP is not well known and the tool support is not well developed. In this paper, taking an example in ET robot contest, we exploit STAMP for the risk analysis of our Mind-Storm robot. Based on the experience, currently we are designing and developing a web-based STAMP tool. This poster reports our progress for the goal.

## 1.　まえがき

近年, システムが大規模・複雑化になり, システム障害もシステムの構成要素のみならず, 構成要素間やシステムと人間との相互作用に起因するものが発生している. そこでSTAMPなど相互作用に着目した分析手法が注目されており, また, そのようなツールにも注目が集まっている. そこでユーザの PC にインストールする必要がなく, どの PC からも同じようにアクセスできる web ベースでの設計に着目した. 本研究では, ロボットコンテストを事例に STAMP でリスク分析を行う. それを基に初めての人でも使える web ベースのツールの設計・開発を行う.

## 2.　STAMP とは

STAMP とは,　現代のシステムのアクシデントの多くは, システム構成要素の故障によって起きるのではなく, システムの中で安全のための制御を行う要素と制御される要素の相互作用が働かないことによって起きるというアクシデントモデルのことである.

例として ET ロボコンの難所の一つであるルックアッ プゲートを分析した. 手順とともに次に示す. まず準備としてアクシデント・ハザード・安全制約の識別と, コ ントロールストラクチャの構築を行う. アクシデントとは, 望んでもいないし計画もしていない, 損失につながるようなイベ ントである。ハザードとは, 環境のある最悪な条件と重なることでア クシデントにつながるような, システムの状態もしくは条件である。安全制約とは, ハザードが認識されると, それらからシステムを安全に保つための要件もしくは制約を意味する.

コントロールストラクチャとは, システムにおいて, 安全制約の実現に関係するコンポーネントおよび, コンポーネント間の相互作用を分析し, 制御構造図として記したものである.

次に step 1 として非安全なコントロールアクション（UCA）の抽出を行う. コントロールストラクチャをベースに, 制御対象のプロセスに対するコントローラーからのアクションのうち, ４つのタイプの安全でないコントロールアクションを抽出し識別する. 次に step 2 として非安全なコントロール（につながるシナリオ）の原因の特定をする. 基本的に, 安全制約を保

Table 1. Identification of Accidents, Hazards, and Safety Constraints

| アクシデント | ハザード | 安全制約 |
|---|---|---|
| ゲートに接触 | 車体が適切な角度まで傾いていない　H1 | 車体が傾くまで走行してはいけない |
| コースアウトする | ライントレースできていない H2 | EV3は常にラインをトレースしなければならない |
| 傾斜時に転倒 | スピードが速い H3 | ゴール後に一定の速度になっている |

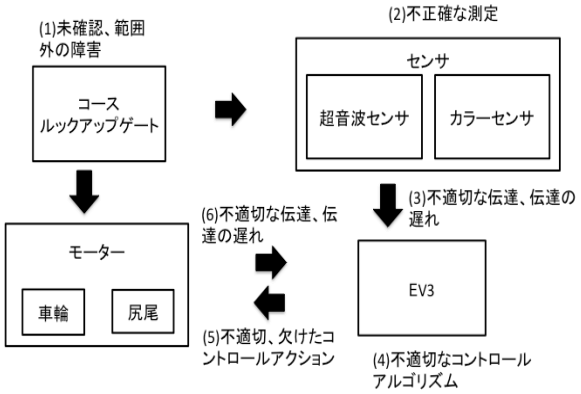


Fig. 1. Control Structure of Mind-Storm Robot

１：日大理工・学部・情報　２：日大理工・教員・情報

つためのコントロールループやその構成要素を確認し，コントロールループに齟齬の原因を 11 つのガイドワードから検討し，原因を抽出する．今回は，11 つのガイドワードのうちコントロールストラクチャに適した 6 つを選択し検討した．次のステップとして UCA に至るシナリオと対策を記述するが，紙面の都合上省略する．

Table 2. Identification of UCA

| コントロールアクション | 与えないとハザード | 与えるとハザード | 早すぎ、遅すぎ、誤順序でハザード | 早すぎる停止、長すぎる適用でハザード |
|---|---|---|---|---|
| 傾く | 超音波センサからEV3に測定結果が伝わらないため、傾かない<br>UCA1 | 超音波センサからEV3に誤った測定結果を伝えたため、傾かない<br>UCA3 | 超音波センサからEV3に測定結果が遅れて伝わるため、ゲートにぶつかる<br>UCA5 | EV3からモーターへのコントロールアクションが早すぎる停止により適切な角度まで傾かない<br>UCA7 |
| | EV3からモーターに命令が伝わらないため、傾かない<br>UCA2 | EV3からモーターに誤った命令がつたわるため、傾かない<br>UCA4 | EV3からモーターに命令が遅れて伝わるため、ゲートにぶつかる<br>UCA6 | |
| 減速 | モーターからEV3に測定結果が伝わらないため、距離が測れず減速できない<br>UCA8 | モーターからEV3に誤った測定結果が伝わるため、任意の場所以外で減速する<br>UCA9 | モーターからEV3に遅れて測定結果が伝わるため、任意の場所以外で減速する<br>UCA10 | |
| 走行 | カラーセンサからEV3に測定結果が伝わらないため、コースアウトする<br>UCA11 | カラーセンサからEV3に誤った測定結果を伝えたため、コースアウトする<br>UCA13 | カラーセンサからEV3に測定結果が遅れて伝わるため、コースアウトする<br>UCA15 | 走行命令が早すぎる停止により、コースアウトする<br>UCA17 |
| | EV3からモーターに命令が伝わらないため、コースアウトする<br>UCA12 | EV3からモーターに誤った命令を伝えたため、コースアウトする<br>UCA14 | EV3からモーターに命令が遅れて伝わるため、コースアウトする<br>UCA16 | 走行命令が長すぎる適用により、コースアウトする<br>UCA18 |

Table 3. Specification of Causal factor

| | (1)未確認、範囲外の障害 | (2)不正確な測定 | (3)不適切な伝達、伝達の遅れ | (4)不適切なコントロールアルゴリズム | (5)不適切、欠けたコントロールアクション | (6)不適切な伝達、伝達の遅れ |
|---|---|---|---|---|---|---|
| 超音波センサからEV3に測定結果が伝わらないため、傾かない<br>UCA1 | | | 超音波センサからEV3への伝達が不適切 | | | |
| EV3からモーターに命令が伝わらないため、傾かない<br>UCA2 | | | | プログラムのアルゴリズムが不適切 | EV3からの不適切なコントロールアクション | |
| 超音波センサからEV3に誤った測定結果を伝えたため、傾かない<br>UCA3 | ルックアップゲートの状態により想定外の測定結果が伝わる | 超音波センサの測定結果が不正確 | 超音波センサからEV3への不適切な伝達 | | | |
| EV3からモーターに誤った命令を伝えたため、傾かない<br>UCA4 | | | | プログラムのアルゴリズムが不適切 | EV3からの不適切なコントロールアクション | |
| 超音波センサからEV3に測定結果が遅れて伝わるため、ゲートにぶつかる<br>UCA5 | | | 超音波センサからEV3への伝達の遅れ | | | |
| EV3からモーターに命令が遅れて伝わるため、ゲートにぶつかる<br>UCA6 | | | | プログラムのアルゴリズムが不適切 | EV3からのコントロールアクションの遅れ | |
| EV3からモーターへのコントロールアクションが早すぎる停止により適切な角度まで傾かない<br>UCA7 | | | | プログラムのアルゴリズムが不適切 | EV3からの不適切なコントロールアクション | |

## 3.　Web ベースツールの調査・比較

web ベースツールの最大の特徴は，機種や OS に依存せずに動作することである．HTML5 に対応したブラウザであれば，すべての機種で機能を発揮し，端末へのインストールも必要ない．このことは，プラットフォームごとに開発する手間がなくなり，開発費用の節約や納期の短縮など時間的なコストの削減に直結するメリットとなる．また，インターネットに接続しているため端末外(クラウド)へデータをバックアップしやすく，端末故障や買い替え時のデータのリストア，複数端末でのデータ共有もしやすい．

一方で，ネット接続が前提となる，機能を多くするほど動作が緩慢になる，利用が短時間に集中した場合にサーバーの負荷が高まりアプリの反応が鈍くなるといったデメリットもある．

## 4.　設計と開発

STAMP の一連の手順を，慣れていない人でも順を追って簡単な操作で行えるように設計した．表にはあらかじめ項目名を設定し，記述する内容を明確化した．また，前の手順で記述した内容を自動的に反映することで，再び入力する手間をなくした．コントロールストラクチャの構築では，ガイドワードを選択形式にすることによって入力ミスをなくした．言語は JavaScript を用いて開発した．

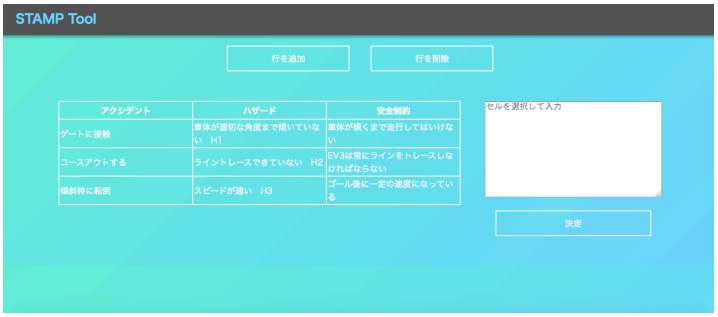


Fig 2. Screenshot of STAMP Tool

## 5.　今後に向けて

本ポスターでは，STAMP の知識がない人でも分析ができることを目的とした，web ベースツールの開発を報告した．今後は，被験者実験を行いツールの有用性や課題を検討する予定である．

## 6.　参考文献

[1] 情報処理推進機構 ：「はじめての STAMP/STPA」, (2016-04)
[2] 狩野祐東：「確かな力が身につく JavaScript「超」入門」, (2015/11/05)