STAMP/STPAを活用したVDM仕様記述の構築

藤崎 淳史[1]　荒木 啓二郎[1]　大森 洋一[1]

概要：近年，IoT や CPS といった複雑なシステムの安全性を検査するために STAMP/STPA の利用が期待されている．しかし，STAMP/STPA は非機能要件に対する安全解析は得意とする一方で，状態やアルゴリズムといった機能的な面の安全解析は得意としない．本研究では，STAMP/STPA の実施に際して形式手法の一つである VDM を活用することで前述した問題を解決できると考え，STAMP のモデルから効率良く VDM の仕様記述を構築する手法を提案する．

1. はじめに

近年，IoT(Internet of Things) や IoT を組み込んだ CPS(Cyber Physical System) を用いた社会インフラが広く浸透していくことが期待されており，今後多くのシステムが IoT や CPS を包含することになると思われる．IoT，CPS といったシステムは，ソフトウェアだけにとどまらずハードウェアや外部環境へ様々な影響を及ぼす可能性が考えられるため，安全性の確保は重要な課題である．

そうした課題を解決するために，システムの相互作用に着目した安全解析手法として STAMP/STPA の活用が期待されている．

STAMP では動的な外部環境も含めたシステムの事故モデルを構築するため，システムの構成要素間の静的な関係から事故を分析するフォルトツリー解析（Fault Tree Analysis:FTA) などよりも IoT や CPS に適している [1][2]．

しかし，STAMP/STPA はメカニズム，技術的問題，人的問題といった非機能的部分に起因する事故を解析することを得意とする一方で，システムの状態遷移やアルゴリズムを厳密に検証する方法は定義されていない．

本研究では，前述した問題を解決するために形式手法の一つである VDM が有効だと考え，STAMP の事故モデルから効率的に VDM の仕様記述を構築する方法を提案する．VDM の仕様記述言語はモデル化対象のシステムの状態を記述することに重点を置いているため，STAMP/STPA で作成したコンポーネントとの対応付けが可能であると考えた．また，最終的に VDM の仕様記述を踏まえた STPA のハザード分析を行なうことで，IoT や CPS などのシステムのさらなる安全性の確保を目的とする．

[1] 九州大学 大学院システム情報科学府 情報知能工学専攻
Faculty of Information Science and Electrical Engineering, Kyushu University

2. STAMP/STPA

本研究では 1 章で述べた問題を解決するため，STAMP のモデルおよび STPA のハザード分析をもとに効率良く VDM の仕様記述を構築する手法を提案し，それらを用いた安全解析を実施する．ここで，STAMP/STPA の実施手順を以下に示す．

- 準備 1 ：アクシデント，ハザード，安全制約の識別
- 準備 2 ：コントロールストラクチャの構築
- STPA パート 1 ：安全でないコントロールアクション（UCA）の識別
- STPA パート 2 ：潜在原因の識別

3. 提案手法

我々は，2 章で述べた手順の準備 2 と STPA パート 1 においてコントロールストラクチャを利用した VDM 仕様記述の構築を考えた．提案する手法の手順は以下の通りである．

(1) コントロールストラクチャの作成
(2) 各コンポーネントのプロセスモデルと状態を想定
(3) コントロールアクションとフィードバックを想定
(4) 各コンポーネントごとにモジュールを想定し，VDM の仕様記述の型定義と状態定義を追加
(5) UCA から仕様記述の不変条件や事前条件，事後条件を抽出
(6) 仕様記述の機能定義を追加
(7) コントロールストラクチャが詳細化可能であれば詳細化
(8) 以上を繰り返し，仕様記述の詳細化を行なう

VDM の仕様記述は抽象度の幅が広く，要求仕様に近いものから実装レベルまで記述することができる．本研究

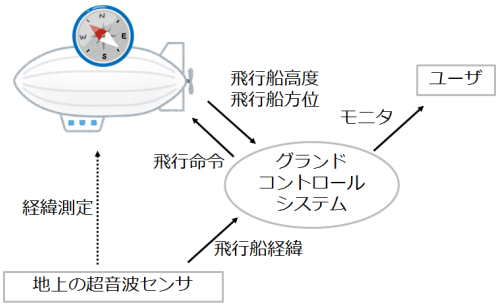

図 1　飛行船システム

ではその利点を活かし，STAMP のコントロールストラクチャの詳細化に合わせて，仕様記述の詳細化を行なう．

4.　適用事例

提案手法の適用事例として飛行船システムを用いた．このシステムを図式化したものを図 1 に示す．

（1）ではまず，図 2 のように抽象度を高く設定したコントロールストラクチャを作成する．

（2），（3）では一般的な STAMP/STPA の準備手順と同じ要領で，各コンポーネントが持つ状態，コントロールアクションとフィードバックを定義する．たとえば飛行船は，内部に自身の情報（高度，方位，経緯）を持ち，飛行船搭載のソナーと角速度センサにより飛行船の高度と方位の計測結果をグランドコントロールシステムにフィードバックする．一方でグランドコントロールシステムでは，センサによって計測された飛行船の情報をを持ち，飛行船に対して「飛行戦略指示」のコントロールアクションを出す．ここまでのコントロールストラクチャを図 3 に示す．

（4）ではここまで作成したコントロールストラクチャをもとに VDM の仕様記述を作成する．各コンポーネントごとにモジュールを作成することで効率良く仕様記述を作成する．適用事例における作成されるモジュールは「グランドコントロールシステム」「飛行船」「地上センサ」「ユーザ」の 4 つである．このうちモジュール「ユーザ」はフィードバックを受けるだけのコンポーネントであり，内部に状態定義もプロセスモデルを持たないと判断し，VDM 仕様記述から除外した．コントロールアクションやフィードバックは，矢印の根本にあたるコンポーネントが機能定義として持つこととすると，たとえばモジュール「グランドコントロールシステム」は内部に状態定義「飛行船情報」と機能定義「飛行戦略指示」「モニタ」を持つ．

（5）では，STPA パート 1 で抽出した UCA から各機能の不変条件や事前・事後条件を記述する．適用事例では，「着陸時に推進する」というハザードに対して「高度が 0 の時に前進後退命令が出される」という UCA が考えられるので，前進後退の命令には事前条件として「高度が 0 の時は前進（後退）しない」という条件が付与される．

（6）において抽象度の高い VDM の仕様記述の雛形を

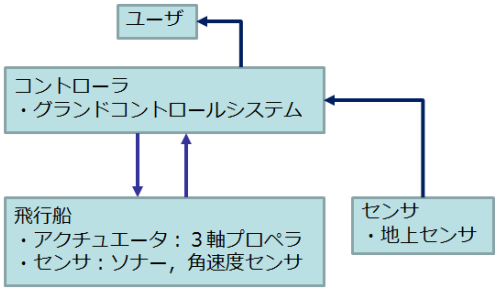

図 2　（1）におけるコントロールストラクチャ

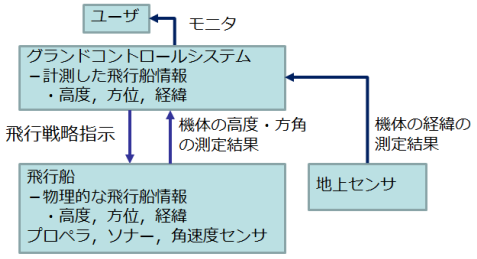

図 3　（3）におけるコントロールストラクチャ

構築する．（7）においてコントロールストラクチャの詳細化が可能ならばさらに詳細化を行ない，併せて仕様記述にモジュールや状態，機能定義を追加する．以降はこれらを繰り返す．適用事例では，今回はコンポーネント「飛行船」の内部に含めていたプロペラ，ソナー，角速度センサをそれぞれ別のモジュールと捉え，さらに機能を付与していく手順を取った．

5.　おわりに

青木ら [4] は，STAMP/STPA によるハザード分析の機能的部分の検証方法としてモデル検査を用いる方法を提案している．これは，システムの状態やロジックを網羅的に検証する点で重要である．しかし，ソフトウェアのモデル検査は検査技術自体の難しさなどの問題点が存在する．

本研究では，STAMP/STPA で得られるコントロールストラクチャから VDM の仕様記述を効率的に構築する手法を提案した．今後は，これら構築した STAMP モデルと VDM の仕様記述を用いて STPA のハザード分析を行い，さらなる安全性の確保を可能にすることを目的とする．

参考文献

[1] Nancy Leveson, “An STPA Primer”, http://sunnyday.mit.edu/STPA-Primer-v0.pdf, 2013.
[2] 八山幸司，“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”，www.jetro.go.jp/world/reports/2015/02/99e8dacaf47e2f91.html，2015.
[3] 独立行政法人 情報処理推進機構，“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～”，www.ipa.go.jp/sec/reports/20160428.html，2016.
[4] 青木善貴，福島祐子，“STAMP/STPA によるハザード分析のモデル検査を用いた支援”，ソフトウェアエンジニアリングシンポジウム 2016，pp.219-226，2016.