5N-01

AADL 活用による安全分析 STAMP/STPA の支援

目黒友貴[1]　大友楓雅[2]　力武克彰[3]　岡本圭史[3]

仙台高等専門学校情報電子システム専攻科[1]　富士アイティ株式会社[2]　仙台高等専門学校[3]

1. はじめに

現在の社会に存在するシステムは以前のシステムと比較してコンポーネントの数が増加し大規模化・複雑化している．このようなシステムはコンポーネント単体の故障だけではなく，コンポーネント間の組み合わせによってシステム全体に不具合が発生するケースに注意が必要である．このような複雑なシステムで発生する不具合は FTA や FMEA などといった従来の安全分析手法では解析が困難なことがある．そのため，複雑なシステムを対象とした新しい安全分析手法 STAMP/STPA が提唱された．[1]

STAMP(System Theoretic Accident Model and Processes)はシステム理論に基づくアクシデントモデルであり，STPA(STAMP based Analysis)は STAMP に基づいた安全分析手法である．STAMP/STPA ではコンポーネント間の相互作用に注目して分析を行うため，コンポーネント間の相互作用によって引き起こされる障害の分析に有効とされている．複雑なシステムにおいて FTA などの従来の安全分析では識別できなかった障害を STAMP/STPA で識別できたという事例が報告されている．[2]

STAMP/STPA の手順[2]を述べる．STAMP/STPA の安全分析でははじめにシステムのアクシデント，ハザード，安全制約を識別する．ここでアクシデントとは損失につながるようなイベント，ハザードはある条件を満たすとアクシデントにつながるようなシステムの状態，安全制約はハザードからシステムを安全に保つための要件もしくは制約である．その後，システムの振る舞いを示すモデルである，図 1 のようなコントロールストラクチャを作成する．コントロールストラクチャを作成する際に安全制約を満たすのに必要なシステムの指示（コントロールアクション）を識別する．それらを用いてシステムに非安全な状態を引き起こす非安全なコントロールアクション UCA(Unsafe Control Action)を識別する．コントロールストラクチャから識別したそれぞれの UCA に関係のあるものだけを抽出し，さらに分析を行い UCA の原因となるハザード要因 HCF(Hazard Causal Factor)を特定する．最後に識別したハザード要因を防ぐようにシステムの改良を検討する．STAMP/SPTA では上記のように分析を行うが，分析を行うにつれ前の作業で気づけなかったことが後の作業を行うことで気づけるということがあるため，基本的には上記の作業を何回も繰り返し行うことで安全分析を行う．

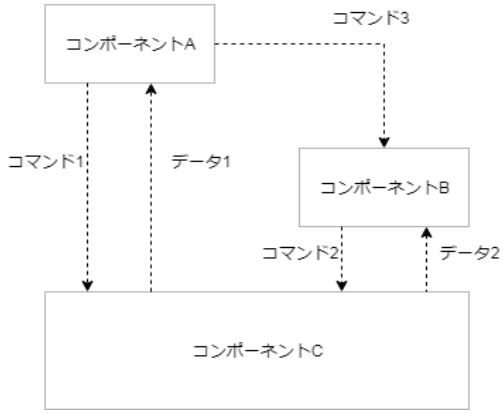

図 1　コントロールストラクチャの例

本研究では STAMP/STPA のさらなる普及のため，STPA 分析にかかる作業量の削減をする方法の提案を行う．

2. 提案手法

STAMP/STPA ではシステムの仕様や設計段階の情報に基づいて安全分析が行える．本研究ではシステムの仕様を基に STAMP/STPA を適用する際のコスト削減のための STPA 支援手法を提案する．

システム開発プロセスでは仕様通りのシステムを開発する必要がある．そのため，システムのプロセスをわかりやすく可視化するためのモデルを作成するモデリングという工程を行う．そのモデリングを実施するためのツールとしてアーキテクチャ記述言語 AADL(Architecture Analysis Design Language)[3]がある．AADL によるモデル作成ではシステムをグラフィカルで表現することが可能となっており，さらに安全分析用の拡張を用いることで作成したモデルで一

部の安全分析を行うことが可能である．本研究では，コントロールストラクチャの構築に開発時に構築される AADL を使うことで，STPA の作業量を削減し，あわせて AADL 拡張を使用した自動的な安全分析も併用することで STPA の結果の充実を目指す．

AADL モデルと言語拡張を利用した安全分析を精査し，AADL モデルに基づく STAMP/STPA の手順を提案する．なお AADL モデルと言語拡張を利用した安全分析では，FIA,FTA を自動的に実行できる．

ハザードを引き起こす複雑な条件をモデルに予め全て含めることは現実的ではないため，複雑な要因に起因するハザードを AADL モデルにより分析支援するのは実用的ではない．一方通常の STAMP/STPA では人間の形式化できない知識や発想を用いることでそのようなハザードを見つけることが可能であると考えられる．そのため，発見するのが比較的簡単なハザードに関しては AADL の言語拡張を用いて自動安全分析を行い，自動で見つけることが困難なハザードに関しては通常の STAMP/STPA を行うことで分析を行う手法が有効であると考えられる．AADL の言語拡張を利用した STAMP/STPA と通常の STAMP/STPA の手順の対応は図 2 に示すとおりである．

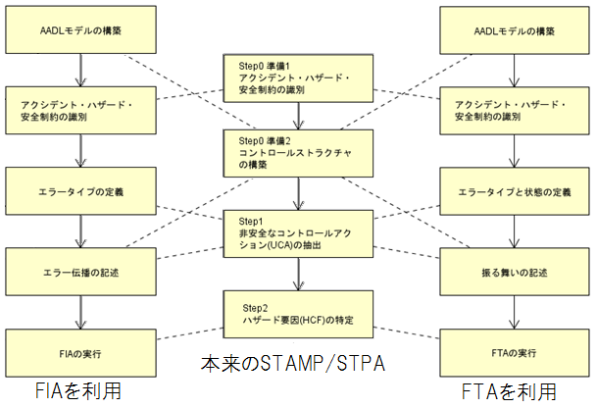

図 2 STAMP/STPA と AADL 利用の安全分析の対応

3. 提案手法の適用

今回は提案手法の有用性を検証するために提案手法を用いて話題沸騰ポット[4]を対象として安全分析を実施した．モデルの抽象度として，本来の STAMP/STPA で使うような抽象度の高いモデルを用いた．

適用の結果，FIA を用いた分析では，単体コンポーネント故障に起因するハザードに関しては分析を行うことが可能であった．また FTA では，比較的条件が簡単なハザード発生に関しては分析できた．しかし，事前に標準の STAMP/STPA で識別していたハザードシナリオ「ポットのお湯の保温温度の設定を低くしようとして誤って保温設定変更ボタンを二度押してしまい，設定温度がユーザーの想定より高くなってしまい，火傷してしまう」は識別できなかった．

後知恵となるが，AADL モデルのコンポーネントの状態遷移に“保温設定ボタンを二回押す”という状態遷移を追加すれば，このハザードシナリオも識別できると考えられる．しかし，予めこのような状態遷移を全てモデルに追加することは現実的ではない．そのため，このような複雑な条件がハザードの発生に関わるものは本来の STAMP/STPA で行うのがよいと考えられる．

4. まとめ

本研究では STAMP/STPA の手順にかかる作業量の削減を目的として AADL を利用した自動分析を援用することを提案した．また，提案手法の有用性検証のため，話題沸騰ポットに対し提案手法を適用した．

AADL を用いた自動分析では，3 章で示した複雑な要因に起因するハザードシナリオ以外のハザードシナリオは識別できた．そのため，AADL を用いて分析が可能な単純な条件で発生するハザードは自動分析を援用し，分析者の知識や発想などが必要な複雑なものは人間が行うことで，分析にかかる作業量を減らすことができ，ひいては分析者が複雑なハザードシナリオの識別に注力できるようになると考える．

【参考文献】

[1] N. Leveson (2011), Engineering a Safer World
[2] N. Leveson (2013), An STPA Primer.
[3] Peter H. Feiler, David P. Gluch(2012),Model-Based Engineering with AADL: An Introduction to the SAE Architecture Analysis & Design Language
[4] 話題沸騰ポット要求仕様書 第７版(2005), SESSAME

「Support of safety analysis method STMAP / STPA by using AADL model」
1「Yuuki Meguro・National Institute of Technology, Sendai College」
2「Huuga Ootomo・Fuji IT Co., Ltd」
3「Keishi Okamoto・National Institute of Technology, Sendai College」
3「Yoshiaki Rikitake・National Institute of Technology, Sendai College