事例報告：AADL を用いた STAMP/STPA 支援

岡本圭史，力武克彰
仙台高等専門学校
{okamoto, yoshiaki}@sendai-nct.ac.jp

大友楓雅
仙台高等専門学校情報電子システム工学専攻
a1602006@sendai-nct.jp

要旨

本稿では，アーキテクチャ記述分析言語 AADL による安全分析手法 STAMP/STPA 支援事例として，特にハザード誘発要因識別の支援事例を報告する．

1. はじめに

複雑化したシステムの安全分析に対応するため，システム理論に基づく事故モデル STAMP(Systems-Theoretic Accident Model and Process)及び STAMP に基づく安全分析手法 STPA(STAMP based Process Analysis)が提唱された[1]. STPA では，ハザードを識別，コントロールストラクチャー（Control Structure，CS）を構築し(Step1)，それを基に，コンポーネント間の非安全制御動作(Unsafe Control Action，UCA)を識別し(Step2-1)，得られた UCA の誘発要因（Causal Factor，CF)を識別する(Step2-2).

STAMP/STPA では分析者の発想に重きを置くことで，従来法では気づきにくい要因に気付きやすくしている．他方 AADL(Architecture Analysis and Design Language)を用いて，人と機械支援の相補的分析の提案[2]や，STPA の一部自動化[3]が行われている．そこで，AADL を用いた STAMP/STPA 支援法の提案を目標とし，AADL による STAMP のモデル化と STPA Step2-2 支援の事例を報告する．

2. STAMP/STPA と AADL

AADL はアーキテクチャ記述・分析言語であり，AADL モデルにアノテーションを追記することで分析が可能になる．安全分析用アノテーションを定義した拡張に Error Model Annex があり，安全分析をツール実行できる．

AADL と STAMP はともにコンポーネントベースであるため，STAMP の CS は AADL モデルとして記述できる[2,3]. また STPA Step2-1 のタイプは Error Model Annex のエラータイプを用いて定義できる．[2]では，Fault Impact Analysis(FIA)を用いたハザード分析を行っている．また[3]では，手動分析と自動分析を組み合わせることで分析結果を充実させるというアプローチを提案している．本稿では，[2]の分析法を STPA の手順に組込み，[3]の提案を試みる．

3. 事例：AADL を用いた CF 識別支援

踏切への STPA 適用事例[4]を参考に CS を AADL モデルとして記述した．さらに FIA を用いて UCA 候補や CF 候補の影響範囲を指摘し，その結果を参考に STPA を実施した．なお FIA を実施するために，Step1 のタイプをエラーソースとして，コンポーネント内やコンポーネント間のタイプ伝搬をエラー伝搬として，AADL モデルにそれぞれ追記した．

STPA Step2 支援に FIA を用いることで，分析対象 UCA を引き起こす CF を識別できた．具体的には，CF の影響範囲に分析対象 UCA が含まれることをツールにより指摘できた．また，CF が別のコントロールループの UCA を引き起こすことも指摘できた．

以下の課題を確認した．1）分析項目に応じた AADL モデル要素の詳細化が必要である．2）Step2-1 支援を実施するには，ハザードへの到達判定が必要となる．しかしハザードはシステムの状態であるため，モデルの改善が必要である．3)FIA は単一要因からの影響範囲のみ指摘可能であるため，複合要因の識別には FIA 以外あるいはモデルの改善が必要となる．

参考文献

[1] Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2011
[2] Procter, S. and Hatcliff, J. An Architecturally-Integrated, Systems-Based Hazard Analysis for Medical Applications, Formal Methods and Models for Codesign (MEMOCODE), 2014
[3] Feiler, P. et al., Improving Quality Using Architecture Fault Analysis with Confidence Arguments, 2015
[4] システム安全性解析 WG，はじめての STAMP/STPA，情報処理推進機構，2016