3G-03

STAMP/STPAに基づくリアルタイム制御システムにおける障害診断の検討

鎌田大貴 * 小林良輔 * 小林幸彦 † 伊藤信行 †
梶克彦 * 内藤克浩 * 水野忠則 * 中條直也 *
愛知工業大学 *
三菱電機エンジニアリング株式会社 †

1 はじめに

リアルタイム制御システムのソフトウェアは複雑化の傾向にあり，生産性の低下や障害原因の特定の困難化などが懸念されている．そのため，システムの安全性・信頼性を向上させる取り組みが必要となる [1]．その一つとして，動作中のシステムのログデータを収集・解析して障害発生の原因を診断するものがある．しかし，コンポーネント故障に基づく障害を想定した分析手法 [2] では複雑化したシステムへの適用が困難である．

そこで，システム同士の相互作用を伴う動作にあるハザードに着目した STAMP(System Theoretic Accident Model and Processes)[3]/STPA(System Theoretic Process Analysis)[4] 手法の適用を検討している．STAMP はシステムを構成するサブシステム間の相互作用に焦点を当て，システム全体の流れを表す事故モデルである．システム設計段階では STPA という障害分析手法を適用することによりハザード分析を行っている．これを運用段階に適用する手法を提案している [5]．そこでは，ACC(Adaptive Cruise Control)[6] をリアルタイム OS を搭載したミニチュアカーに組込み，提案手法を用いたリアルタイムな障害診断を検討している．本研究では新たなハザードと制約条件の識別を行いリアルタイム性を検証した．

2 提案手法

本研究では，リアルタイム制御システムの障害監視のための STAMP/STPA の適用を提案する．STAMP/STPA 手法を応用して設計段階ではなく運用段階に適用する．手順は以下の通りである．(1)〜(3) は STAMP/STPA 手法を適用し，(4) でリアルタイム監視を実現する．

(1) 想定されるシステムの障害

(2)Control Structures の構築 (図 1)

Control Structures は，システムの制御構造であり，システムに関係するサブシステムと制御アクションを識別して可視化したものである．

(3) ハザードの識別

可視化した制御アクションに潜むハザードをガイドワードを用いて識別する．ガイドワードは以下の 4 つである．

- 不必要な制御アクションの供給
- 不適切な制御アクションの供給
- 意図しないタイミングでの供給
- 制御アクションが途中で停止

(4) 制約条件の識別と監視

(3) で識別したハザードを検出するための制約条件を識別する．識別した制約条件を監視する事でハザードを検出する．検出時にはバッファにハザード検出のログを書き込む．

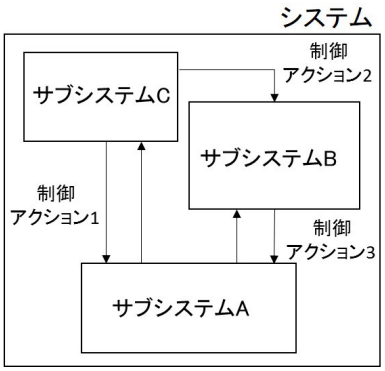

図 1: Control Structures

3 実験

本章では実験について述べる．実験の目的は，ハザード監視のリアルタイム性について検証することである．

3.1 実験機器

実験機器として用いる ZMP 社のミニチュアカー RoboCar 1/10 for Automotive Platform(以下，RoboCar とする) を採用した．リアルタイム制御システムとして，ACC を採用した．ACC とは，測距センサにより先行車との車間距離を検知し，一定の車間距離を保ちながら追従走行をするシステムである．本研究では，ACC を RoboCar に搭載したうえで実験を行うものとする．

*Study of Fault Diagnosis on STAMP/STPA for Real-time Control System Hiroki Kamata Ryosuke Kobayashi Yukihiko Kobayashi Nobuyuki Ito Katsuhiko Kaji Katsuhiro Naito Tadanori Mizuno Naoya Chujo Aichi Institute of Technology Mitsubishi Electric Engineering Co., Ltd.

3.2 提案手法適用

ACC に関係するサブシステム間の制御アクションを識別するために図 2 の Control Structures を展開する．そして図中の制御アクションのハザードを識別する．それらを検出するための制約条件も同時に識別する．今回は，赤外線測距センサと速度制御サブシステム間の距離情報を送信する制御アクションでのハザード，制約条件を表 1 として識別した．

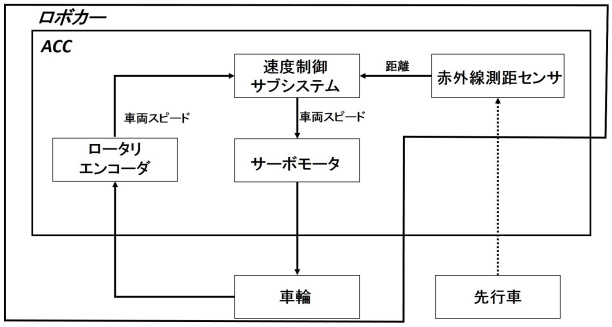

図 2: ACC の Control Structures

表 1: 距離情報のハザードと制約条件

ガイドワード / ハザード / 制約条件	不必要な制御アクションの供給	不適切な制御アクションの供給	意図しないタイミングでの供給	制御アクションが途中で停止
ハザード	センサから、速度制御サブシステムに距離情報が送られない	センサから、速度制御サブシステムに誤った距離情報が送信される	センサから、速度制御サブシステムへの距離情報の送信が遅れる	一定周期で距離情報を送信していたが、送信が中断される
		前方車両がいないが距離情報が送信される		
制約条件	・センサのフラグ状態 ・速度制御サブシステムのフラグ状態	・センサ値の時間的遷移 ・センサ値の空間的遷移	・センサ値の送信周期	・センサ値の送信周期

3.3 実験手順

今回は表 1 のセンサ値の時間的遷移，センサ値の空間的遷移，センサ値の送信周期の制約条件の監視を行った．例としてセンサ値の時間的遷移について示す．ハザードを検出するために故障を注入する．発生したハザードがリアルタイムに監視出来ているかの検証を行う．実験は以下の手順である．

(1) ハザードを引き起こす故障を定義

RoboCar の最大スピードは 2.8m/sec であり，赤外線測距センサの送信周期は 100msec である．このことから 100msec の間に 0.28m 以上離れる事はない．そのため先行車が 100msec 間に 0.28m 以上移動した場合にハザードを引き起こす故障と想定する．

(2) ハザードを引き起こす故障の注入

故障注入では先行車を 0.1 秒間に 40cm 移動させる．この操作によって障害注入する．

(3) 制約条件の監視

センサ値の時間的遷移を監視し，ハザードの検出がセンサ値の送信周期 (100msec) 内であるかどうか確認した．

3.4 実験結果

実験では，センサ値の時間的遷移の制約条件を監視した．表 2 はセンサ値の時間的遷移である．このハザード監視に要する時間は検出前には最大 6μsec だったが，検出時にはバッファにハザード検出のログを書き込むため 14μsec まで上昇した．しかし，センサの送信周期内でハザード監視ができたため，今回実験した範囲では，リアルタイム性が確保出来たといえる．

表 2: 0.1 秒毎のセンサ値の時間的遷移

時刻 [sec]	車間距離 [m]	監視に要する時間 [μ sec]	ハザード検出有無
0.0	0.203696	5.0	無
0.1	0.207810	6.0	無
⋮	⋮	⋮	⋮
19.9	0.213988	5.0	無
20.0	0.572580	14.0	有

4 おわりに

本研究では，リアルタイム制御システムにおける障害監視のための STAMP/STPA を適用する手法を提案した．ACC システムに提案手法を用いてハザードと制約条件を識別することができた．

実験では，リアルタイム制御システムとして ACC を搭載した RoboCar を使用し，STAMP/STPA を適用した．このシステムの赤外線測距センサに故障注入し，ハザード監視を行った．実験結果からセンサ値の時間的遷移のハザードがリアルタイムに監視できたことがわかった．

参考文献

[1] 阪田史郎，高田広章，組込みシステム，オーム社，pp. 1-24 (2011).

[2] 北川裕貴，辻田和宏，山下昭裕，伊藤信行，小林幸彦，水野忠則，中條直也，リアルタイム制御システムにおける故障診断のためのログデータ収集，WiNF2014 (2014).

[3] Nancy G. Leveson， Engineering a Safer World，The MIT Press，pp. 89-93 (2011).

[4] Nancy G. Leveson， Engineering a Safer World，The MIT Press，pp. 211-249 (2011).

[5] 小林良輔，鎌田大貴，伊藤信行，小林幸彦，梶克彦，内藤克浩，水野忠則，中條直也，STAMP/STPA に基づく制御システムのリアルタイム障害監視に関する検討，情報処理学会第 77 回 MBL 研究会，MBLWiP-14 (2015).

[6] 小口泰平，ボッシュ自動車ハンドブック， 日経 BP 社，pp. 1214-1218 (2011).