様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　８　月　３０　日現在

機関番号：　３３９０３
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３００７４

研究課題名（和文）リアルタイム制御システムのための適応的ログ収集エージェントの研究

研究課題名（英文）Research on adaptive log collection agent for real time control system

研究代表者
中條　直也（CHUJO, Naoya）

愛知工業大学・情報科学部・教授

研究者番号：３０３９４４９８

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究では，リアルタイム制御システムのための適応的なログ収集を行うエージェントの基本的な検討と実証を行った．対象となるリアルタイム制御システムとしてアダプティブ・クルーズ・コントロール（以下 ACC)を取り上げた．
まず，ACC搭載車のデータ計測による正常モデルの作成と，外れ値検出による異常検出を行った．実験では機械学習によって高い正答率で異常時を識別できた．多様な信号に対する正常モデル作成は本研究の課題として残された．また，適応的なエージェントによるリアルタイムのログデータ収集を行った．ログ収集のオーバーヘッドは予測可能であり，制御タスクに対して十分小さかった．

研究成果の概要（英文）：In this research, agent system that performs adaptive log data collection for real-time control system were examined and demonstrated. Adaptive Cruise Control (ACC) was used as the real-time control system.
We made normal data models by measurements of ACC-equipped vehicles and detected abnormalities by detecting outliers. In the experiment, the detection system by machine learning could identify the outliers with high correct answer rate. The automatic generation of normal models for various signals remains as a future problem. In addition, real-time log collection by adaptive agents was examined. The log collection overhead is predictable and found to be small enough compared to the control task.

研究分野：　組込みシステム

キーワード：　リアルタイム　システム　制御　ソフトウェア　ログ　障害診断　機械学習　エージェント

１．研究開始当初の背景

産業機器だけでなく民生機器として利用される組込み機器が多数利用されるようになっている．その多くはリアルタイム制御システムであり，自動車などでは事故により人命が損なわれることがあり，高い信頼性が求められている．そのため，リアルタイム制御システムの信頼性を向上させることは重要なテーマとなっている．

一方，リアルタイム制御システムはコンピュータの性能向上に伴って，大規模化，ネットワーク化の傾向にある．この傾向はシステム障害時の原因特定を困難にし，システムの安全性・信頼性を低下させる懸念がある．そのため安全性・信頼性を向上させる取り組みが必要である．

信頼性向上の手段としては，製品の開発段階での設計品質の向上，検証なども重要である．しかし，本研究では障害時に障害原因の箇所を特定する適切なログデータ収集を取り上げる．

障害箇所や原因の診断については，システム動作中のログデータを収集・解析して障害発生の原因を特定することが重要である．しかし，リアルタイム制御システムではログデータを適切に収集する手法に関する研究はあまりなかった．障害が発生した旨のイベントやその障害内容，発生時刻などを記録する機構は実用化され利用されている．しかしながら，複雑化したシステムの障害原因を解析するための適切なデータが記録されていないという問題があった．

２．研究の目的

本研究の目的は大規模なシステムを対象とした信頼性向上である．そのためにリアルタイム制御システムのための適応型のログ収集エージェントの研究を行う．まず，システムが置かれた動作環境で正常時の動作モデルを作成する．次に，テスト中や動作中に障害が検出された場合は障害と論理的な関係を持つ内部の制御データや入出力デバイスなどの情報を対象として，リアルタイムの時間制約を守りながら，適切なログデータを収集する．

３．研究の方法

以下の３つの項目の研究を行った．図１に研究の枠組みを示す．

(1) データ収集に基づく正常モデルの作成と外れ値の検出
(2) 大規模システムを想定したサブシステム間のログデータ収集
(3) サブシステム内のリアルタイム制御システムのログデータの収集

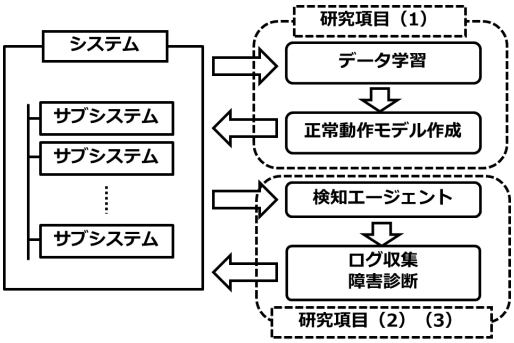


図 1: 本研究の枠組み

(1) では制御システムの記録データに基づく正常モデルの自動作成と，そこからの外れ値の検出による障害検出手法について検討を行う．対象として運転支援システムである ACC (Adaptive Cruise Control)を対象として取り上げる．図 2 に示すように走行中の自動車から ACC の制御用データを取得し，それをもとに正常モデルを作成する．作成した正常モデルを実際に運用されているシステムのデータと比較する．そのモデルから外れた値を外れ値とし，外れ値を検出した場合，障害の可能性を疑い診断につなげる．

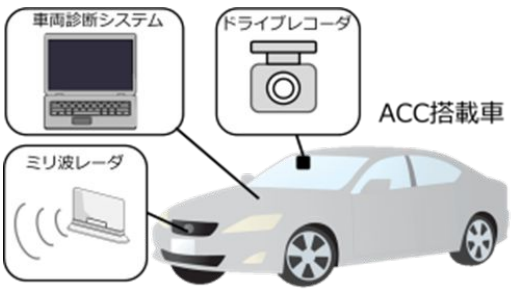


図 2: ACC 制御データの収集方法

(2) では大規模なシステムを想定し，それを構成するサブシステム間の相互作用に着目し，STAMP/STPA に基づいてリアルタイムのログデータ収集によって，異常検出を行う研究を行った．より大規模なシステムへの適用のため，システムの構成要素間の相互作用に注目したアクシデントモデルと解析手法である STAMP/STPA (Systems Theoretic Accident Model and Process, STAMP based Process

Analysis)に注目し，これに基づいたリアルタイムログ収集手法の提案と評価を行う．

表 2 に本研究で使用する STAMP/STPA と FTA（Fault Tree Analysis，故障木を用いた解析）の比較を示す．ここではシステムの解析では STAMP/STPA を使用し，満たすべき制約条件をエージェントタスクとして実装した．実験システムとして自動運転用の各種のセンサーを実装した 10 分の 1 の模型自動車 RoboCar を使用した．図 3 に示す RoboCar は実際の車載制御システムで使用される MPU と OS を備えている．これに ACC を実装して評価を行う．

(3) では個別の制御システム内部の故障や劣化による異常を対象として，正常モデルからの逸脱の検出を FTA（Fault Tree Analysis，故障木解析）に基づいた情報を用いて，リアルタイムのログデータ収集によって，異常検出を行う研究を行う．評価用に(2)と同じ模型自動車を実験システムとして使用する．

表 1: STAMP/STPA と FTA の比較

	STAMP/STPA	FTA
分析対象	システム	サブシステム
事故モデルと手法	サブシステムの振舞いやサブシステム間の相互作用がシステムの安全制約を違反	システム障害であるトップ事象の要因を故障木で解析
分析ツール	Control Structures	FT (Fault Tree)
考え方	ボトムアップとトップダウンの中間	トップダウン
利点	詳細設計前の段階でハザード分析が可能 サブシステムに故障や問題がなくても発生するハザード分析	システム障害宵ウインを論理的に分析でき，障害に至る因果関係が識別できる

表 2: 実験機材の仕様

	RoboCar® 1/10 for AP
CPU	V850E2/FG4 80MHz
RAM	80KB
搭載OS	TOPPERS/ATK2 (AUTOSAR準拠)
サイズ	429.0 * 195.0 * 212.2 [mm]

4．研究成果

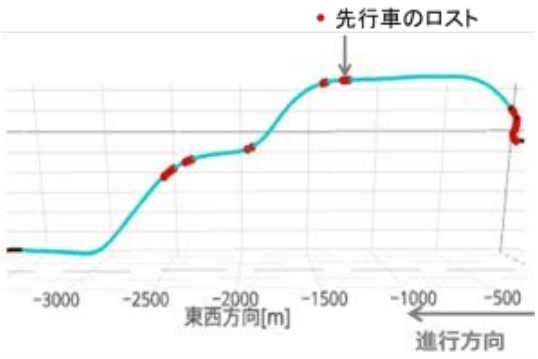
3 つの項目の研究成果について述べる．

(1) データ収集に基づく正常モデルの作成と外れ値の検出

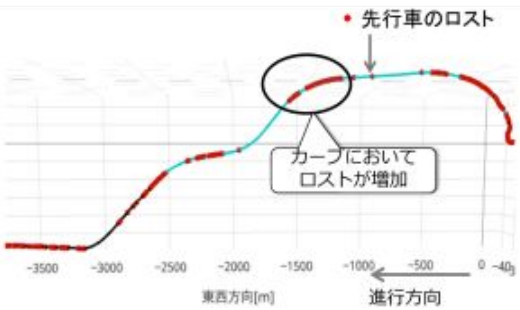
実車の ACC システムでログデータ計測を行い，正常走行モデルを自動的に作成する手法について検討を行った．一定速度で走行する先行車に対し，ACC システムを動作させた車両を追従走行させて，先行車の検出とロスト，車間距離，車速，GPS による 3 次元位置などのデータ計測する実験を行った．また，故障注入として先行車を検出するミリ波レーダを部分的に遮蔽して，同様のデータ計測を行った．図 4 に上方から見た走行経路と，ACC による先行車のロストによる外れ値を示す．図 4(a)は正常時を，図 4(b)は故障注入時を示す．水色の経路上の赤い点は ACC が先行車をロストしていることを示す．図 4(b)に示すように故障注入時にはカーブなどでロストするケースが増加している．

SVM を用いた機械学習によって正常時と故障注入時を識別できるか実験を行った．その結果，平均正答率 94%と高い割合で外れ値を識別できることが分かった．正常時にも先行車のロストが発生するため誤識別する可能性は残っている．しかしながら，全体として高い確率で外れ値を識別でき，システムの障害を検知することが示された．

一方，制御データごとに分布などの性質が異なり，データ学習による正常モデルは一律の方法では作成が難しいことが分かった．大まかな信号カテゴリーごとに，正常モデル作成と外れ値の検知方法が必要と思われる．



(a) 通常時



(b) 故障注入時

図 3: 走行経路と先行車ロスト状況

(2) 大規模システムを想定したサブシステム間のログデータ収集

STAMP/STPA の考え方に基づいて ACC システムをコンポーネントに分解し，図 5 に示す制御構造図(Control Structures)を作成した．

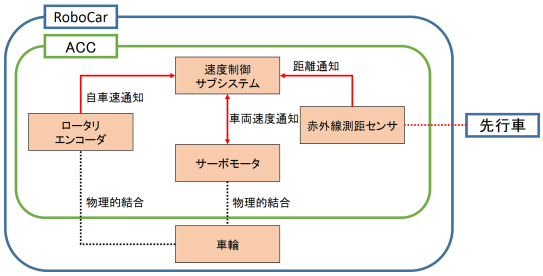


図 4: ACC の制御構造図

また，図 5 で示すように制御構造図を解析し，ガイドワードによりハザードを識別した．そして関連するログ収集用のエージェントタスクを実装した．実験評価用システムとして，模型自動車 RoboCar を使用した．

レーダ信号データの異常などを想定した故障注入を行って，ログデータ収集を行った．ログ収集エージェントによるオーバーヘッドは最大 14 µsec と小さかった．このため制御システムに影響を及ぼさない．またエージェントタスクのオーバーヘッドは設計時に予測可能であり，制御タスクに影響なく故障を含むログデータを収集できることが分かった．

(3) サブシステム内のリアルタイム制御システムのログデータの収集

制御システムを対象として FTA に基づいてエージェントタスクでリアルタイムでのログ収集を行う手法を LoFTE（Log data collection using Fault Tree Expansion）手法として提案した．個別の制御システムとして模型自動車 RoboCar を取り上げ，内部の故障や劣化による異常を対象とした．

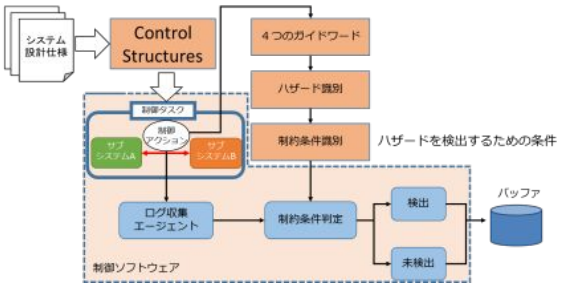


図 5: 制御構造の解析とタスク設計

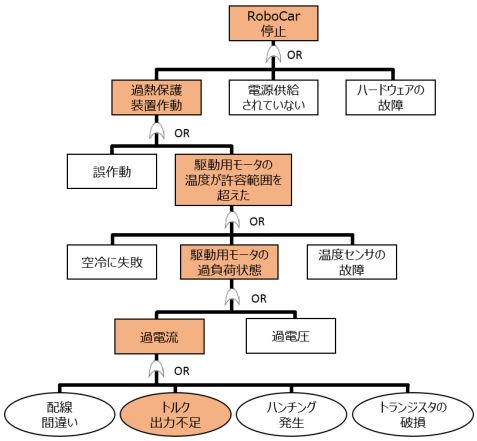


図 6: RoboCar 停止に関する FT

例として図 6 に RoboCar の停止に関する FT（Fault Tree，故障木）の例を示す．ハッチングされた要素は，トルク出力不足によって RoboCar の停止が引き起される経路を示している．作成した FTA に基づいて作成した正常時動作モデルからの逸脱時，

図 7 に示すような RoboCar を使用した実験評価用システムを開発した．

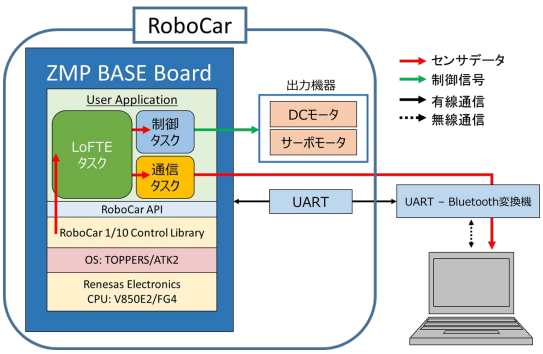


図 7: 評価用の実験システム

評価実験では RoboCar のサーボモータに大電流を流し，それによる加熱保護装置が動作して停止するようにした．この際，ログタスクが過電流，過熱保護，モータ停止という事象の遷移を示す関連エラーコードをリアルタイムでログ収集できた．また，制御タスクは 100msec 周期で動作した．ログ収集のエージェントタスクの実行時間は障害発生前 4 µsec，障害発生時 149 µsec であり，制御タスクの周期にはほとんど影響しない．

これらの解析からエージェントタスクによって障害原因の特定につながる適切なログデータ収集ができた．またオーバーヘッドとなるログタスクの実行時間は，制御タスクの周期と比較して十分に短く，システム制御周期

にほとんど影響しないことが分かった．制御タスクに対するエージェントタスクのオーバーヘッドは設計時に予測可能であり，制御タスクの周期に対して十分小さくできる．

以上で述べたように，リアルタイム制御システムのための適応的ログ収集を行うエージェントに関して，(1)データ収集に基づく正常モデルの作成と外れ値の検出，(2)大規模システムを想定したサブシステム間のログデータ収集，(3)サブシステム内のリアルタイム制御システムのログデータ収集，に関して検討を行い，実験システムと評価を行った．

(1)では作成した正常モデルにより外れ値を適切に検出できることが示された．一方，多様な信号カテゴリーに対しての正常モデルの作成は本研究の課題として残された．

(2)(3)では，サブシステム間の相互作用を伴うシステムではSTAMP/STPAに基づく手法が，システム内の詳細な制御データに関してはLoFTE 手法が有効であることが示された．両手法ともエージェントタスクのオーバーヘッドは設計時に見積り可能であり，制御タスクに比べて小さく抑えることができる．

５．主な発表論文等

〔雑誌論文〕（計　１件）

① Naoya Chujo，Akihiro Yamashita，Nobuyuki Ito，Yukihiko Kobayashi，Tadanori Mizuno, Log Data Collection of Real-time Control System using Fault Tree Analysis, International Journal of informatics Society (IJIS)，No. 8 (2016)，査読有

〔学会発表〕（計　７件）

① 小椋翔太，尾坂啓宏，伊藤信行，梶克彦，内藤克浩，水野忠則，中條直也:運転支援システムのための SVM を用いた外れ値検出の検討，情報処理学会第 79 回全国大会,自動運転・運転支援, 1V-04, 2017 年 3 月 21 日，名古屋大学（愛知県名古屋市）

② 尾坂啓宏,小椋翔太,伊藤信行,梶克彦,内藤克浩,水野忠則,中條直也: 運転支援システムのためのデータ学習による外れ値検出の検討，情報処理学会 ＭＢＬ 第 81 回研究発表会, MBLWiP-17, 2016 年 12 月 7 日，金沢湯涌温泉かなや（石川県金沢市）

③ 古田善蔵,中條直也,本田晋也,倉地亮,早川代祐: Linux を用いた自動運転向けアーキテクチャのリアルタイム性評価，平成 28 年度電気・電子・情報関係学会東海支部連合大会，E1-2，2016 年 9 月 7 日，豊田工業大学（愛知県豊田市）

④ 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, 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, 情報処理学会第 78 回全国大会，3G-03 ，2016 年 3 月 11 日，慶応大学（神奈川県横浜市）

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，リアルタイム制御システムの障害監視のための STAMP/STPA の適用検討，情報処理学会 MBL 第 77 回研究発表会，MBLWiP-14, 2015 年 12 月 2 日，ホテル金泉閣（愛知県豊田市）

⑥ Naoya Chujo，Akihiro Yamashita，Nobuyuki Ito，Yukihiko Kobayashi，Tadanori Mizuno，Real-time Log Collection Scheme using Fault Tree Analysis, Proceedings of International Workshop on Informatics (IWIN2015), pp. 109-114 ，Sep. 7, 2015，アムステルダム（オランダ）

⑦ 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」.第 12 回情報学ワークショップ WiNF2014,要素技術とアルゴリズム,pp. 158-164 ，2014 年 11 月 29 日（土），静岡大学（静岡県浜松市）

６．研究組織

(1) 研究代表者

中條　直也（CHUJO，Naoya）

愛知工業大学・情報科学部・教授

研究者番号：30394498

(2) 研究分担者

水野　忠則（MIZUNO，Tadanori）

愛知工業大学・情報科学部・教授

研究者番号： 80252162

(3) 研究協力者

伊藤　信行（ITO，Nobuyuki）

三菱電機エンジニアリング・駆動制御部・部長

小林　幸彦（KOBAYASHI，Yukihiko）

三菱電機エンジニアリング・制御技術部・主査