愛総研・研究報告
第 18 号　2016 年

リアルタイム制御システムのログデータ収集に関する研究

Study on Logging Method for Real-time Control System

中條直也†，伊藤信行††，小林幸彦††，梶　克彦†，内藤克浩†，水野忠則†
Naoya Chujo†, Nobuyuki Ito††, Yukihiko Kobayashi††, Katsuhiko Kaji†,
Katsuhiro Naito†, Tadanori Mizuno†

Abstract The increasing complexity of embedded systems cause difficulties in locating faulty components or modules. In this report, we present a logging method of real-time control system using fault tree. Two experimental systems have shown that data related to faulty components are collected and overhead for logging is predictable.

1. はじめに

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，医療機器や自動車では人命が関わることがあり，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．また，リアルタイム制御システムのソフトウェア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[1].

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，試験段階での検証などが挙げられる．また，障害発生時に障害箇所を特定した上で対処を行うことで障害の少ないシステムを実現する手段も重要である.

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においてログデータを収集手法に関する研究はあまりなかった．組込みシステムや制御ソフトウェアの障害に関するログとしては，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が多い.

†愛知工業大学情報科学部情報科学科（豊田市）
††三菱電機エンジニアリング（春日井市）

例えば自動車における故障診断機能では異常発生時の基本的な車両状態のデータを収集する[2]．しかし基本的なログデータだけでは，障害がどのような処理や制御の過程で，何が原因で発生したのかを診断することが難しい.

そこで本研究では，リアルタイム制御システムの信頼性向上のためのログデータの収集手法について提案する．設計段階で実施する Fault Tree Analysis[3]（以下 FTA）に基づいて，障害に関連するデータとソフトウェアモジュールを特定しておく．障害発生時には，独立タスクがログデータを収集する．これによって障害が発生した場合に，関連するログデータを収集して解析することで，障害原因の絞込みが容易に行えるようになる.

以降，第 2 章で関連研究として自動車の故障診断機能について述べる．第 3 章では提案手法を述べ，続く第 4 章では提案手法を用いたログデータ収集の実験について述べる．第 5 章でまとめと今後の課題とする.

2. 関連研究

本章ではリアルタイム制御システムにおけるログデータ収集の事例として，自動車の故障診断機能を紹介する.

2.1　自動車の故障診断機能

自動車の制御用のコンピュータは，ECU (Electronic Control Unit)と呼ばれ，ネットワークで

接続され車両制御を行っている．障害発生を検出した時，障害に関係するセンサや診断する項目をコード化した障害コードと車両の状態データを合わせて記録する．障害時のデータをフリーズフレームデータ（以下 FFD）という．このデータは図 1 に示す障害診断装置で読みだすことができる．典型的なシステムでは障害時の FFD に加えて，0.5 秒周期で記録される車両状態データが利用できる．しかし，障害コードと FFD，車両状態では情報が不十分である．システム複雑化に伴って障害原因の診断が困難となる場合が予想される．そこで，障害原因の診断には発生する障害に関連するログデータを数多く収集することが求められる．

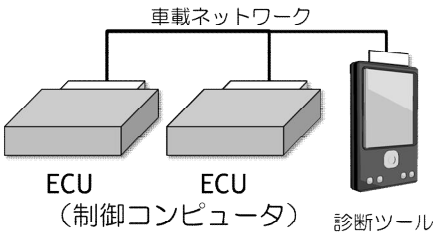

図 1：自動車の障害診断装置[1]

3. 提案手法

本章では，フォールトツリー解析に基づくログデータ収集手法について述べる[4]．想定する障害に対してフォールトツリー(以下 FT: Fault Tree)を用いて，収集するログデータを特定するため，本手法を，LoFTE(Log data collection using Fault Tree Expansion) と呼ぶ．

3.1 提案するログデータ収集機構

本研究で提案するログデータ収集機構は，障害発生後に障害箇所を特定し，一定周期間ログデータを収集し続ける．システム設計段階とシステム運用段階でそれぞれ以下のような手順を取る．

システム設計段階

1. システム設計仕様からの FTA の実施
2. FT で収集すべきデータの指定
3. 指定データのアドレスと収集スケジュールの決定

システム運用段階

1. 制御タスクで発生した障害の特定
2. 障害情報のログデータ収集タスクへの通知
3. 障害に対応したデータをスケジュールに基づきログデータとして収集

図 2 を使って考え方説明する．システム設計段階での FTA の結果を，FT-fl ，FT- f2…として保持しておく．障害 f2 が発生したとき，ログデータ収集タスクにこの情報を通知する．通知を受け取ったログデータ収集タスクは FT-f2 で示されるログデータを収集する．これにより，障害発生時のログデータと周期的に収集したログデータを比較して障害原因の診断を行う．提案手法は，図 2 は提案する LoFTE 手法の概要である．

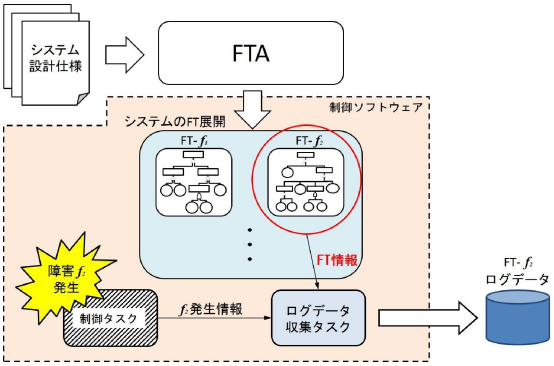

図 2：LoFTE 手法の考え方

3.2 障害箇所と収集ログデータ

適切なログデータ収集を実現するには，障害に対し事前に収集するログデータを決定しておく必要がある．障害箇所と収集するログデータを特定は FTA に基づいて定める．想定障害に対して FT を用いて，収集するログデータを特定しておく．また，現在の制御ソフトウェアは多数のソフトウェアモジュールから構成されるため，FT 内で対応するモジュール毎のログデータを収集することになる．それぞれのモジュールで収集するログデータを予め決定する．

4. 実験

提案手法を定量的に評価するための実験を行う．実験では，通信システムと，自動車を想定したシステムの 2 つを取り上げて，提案手法を実装して評価を行う．

4.1 通信システムで想定する障害事例

医療機器の中にはサーボモータを搭載しているものがあり，サーボアンプと機器が通信して制御している．ここではこのサーボアンプと制御ソフトウェアの通信を行う部分に着目して，障害関連のログデータ収集を行う．

障害事例は制御コマンドデータ送信時にサーボアンプが応答せず通信がタイムアウトすると想定する．制御ソフトウェアの通信部分のモジュール構成を図 3 に示す

図 4 は，サーボアンプとの通信障害につながる事象を記述した FT とそれに関連するモジュール構成を示した図である．図 4 のグレーの部分は想定する通信障害に関連する箇所である．点線で囲まれた部分は，それぞれ個別のモジュールを示している．この障害の事例では３つのモジュールでログデータを収集する．

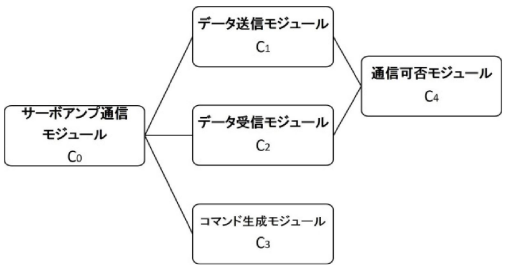

図 3：想定するモジュール構成

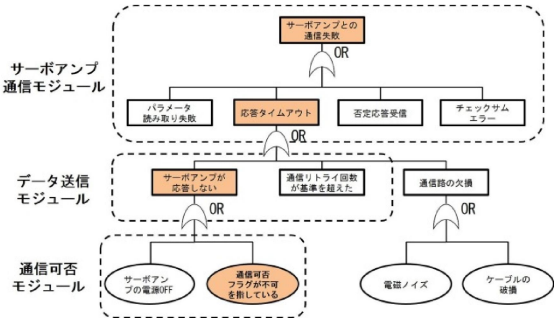

図 4：通信障害に関する FT と関連モジュール

4.1.2　実験方法と結果

ここでは上記の通信障害における事例を取り上げて，図 5 に示すようにリアルタイムで制御する通信システムを実装した．障害としてデータ送信時にタイムアウトする事例を再現した．対象となるデータ送信制御タスクの基本実行周期は 20msec である．提案手法の LoFTE タスクは障害発生時に通信タスクおよび RAM からログデータを収集する．その後，RS-232C 通信を通じてモニタするコンピュータへログデータを転送する．

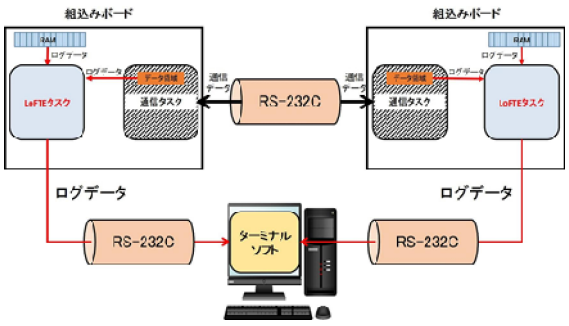

図 5：実験に使用した通信システム

実験機器として CPU ボード KED-SH101[5] とその拡張ボード EXT-102 を用いた．また図 6 にソフトウェア構成を示す．

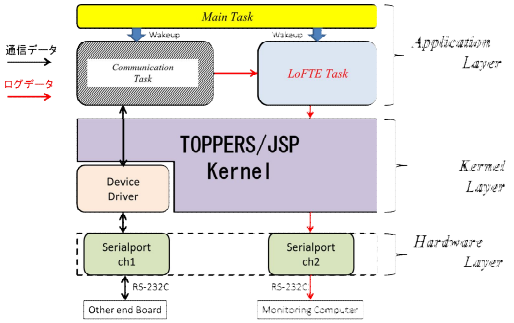

図 6：CPU ボード上のソフトウェア構成

表 1 に収集例のログデータとその内訳を示す．モジュール名は障害を検出したモジュールを示し，データ量は全体で 39 バイトであった．

ログ収集にかかった時間は 1msec であった．他の障害のケースでログ収集時間は同じであった．通信の実行周期の 20msec と比較してログ収集に伴うオーバーヘッドは小さくできることが分かった．また，障害時も通常の周期収集時もこのログ収集にかかる時間の差は出なかった．

表 1：収集ログデータ量

項目名	バイト数
モジュール名	9
エラーコード	4
レジスタ値	1
送信データ	17
リトライ数	4
記録時刻	4
合計	39

4.2　模型自動車を用いた実験

この実験では ZMP 社の RoboCar 1/10 for Automotive Platform[6]（以下，RoboCar） を使用して実験を行う．LoFTE 手法を障害監視に応用し，障害診断のためのログデータ収集の有効性について評価する[7]．またログデータ収集に必要な時間を計測し，リアルタイム性について評価を行う．

4.2.1　RoboCar で想定する障害事例

この実験では RoboCar が異常停止したことを障害事例として想定した．RoboCar を右回りに走行させ手で走行を妨害する．こうすることで，RoboCar は前進を命令しているにも関わらず，前進しないため障害が発生する．

図 7 は，RoboCar の異常停止につながる事象を記述した FT である．グレー部分は想定する RoboCar 停止の障害に関連する箇所である．

4.2.2　実験方法と結果

RoboCar はカーロボティクス分野における研究，教育用のプラットフォームとして開発された四輪自動車型のロボットである．各種センサとアクチュエータを備えており，自動車で使用されるマイコン V850 と，自動車用 OS を搭載している．図 8 に RoboCar の外観図を示す．

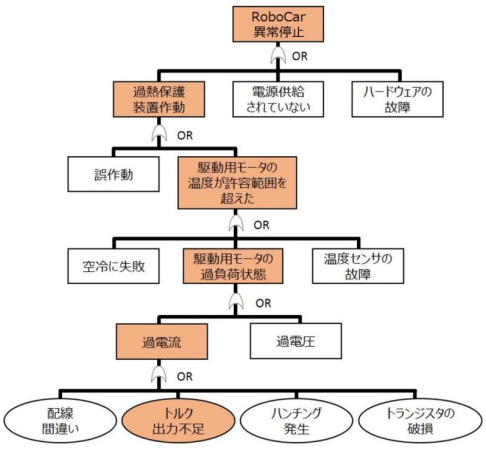

図 7：RoboCar 停止に関する FT

また図 9 に，ソフトウェア構成を示す．走行制御の実行周期は 100msec で動作させている．実験開始から 4 分後に手で RoboCar を停止させて障害を発生させて，ログデータの収集を行った．

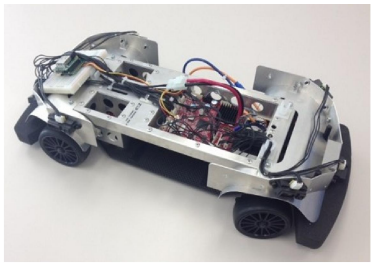

図 8：RoboCar 外観

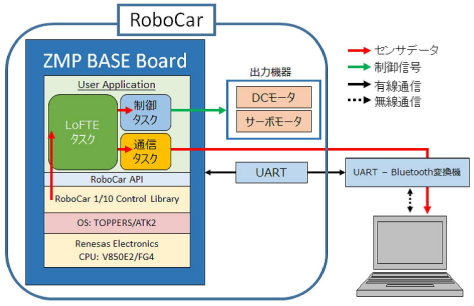

図 9：RoboCar のソフトウェア構成

表 2 に実験結果を示す．　ログデータ収集にかかった時間は，通常走行時 4～4.5μsec で，障害発生時 124－149 μsec であった．障害発生時のログ収集のオーバーヘッドは，走行制御の実行周期の 100mse と比較して小さくできることが分かった．障害時のログ収集にかかる時間は，通常時に比べてログ収集にかかる時間は長くなる．しかしながら，収集ログ量に応じて時間が長くなることが分かった．LoFTE タスクのオーバーヘッドをあらかじめ見積もることが可能である．

表 2：収集されたログ情報

	検出時刻	モータ電流(A)	モータ制御用FET温度(℃)	駆動速度左後輪(m/sec)	駆動速度右後輪(m/sec)	処理時間(μsec)
通常走行時（平均）	0.0秒から3分59.6秒	2.5	49.5	0.8	0.6	4.5
走行停止時	3分59.7秒	7.7	50.5	0.3	0.0	4
過電流	4分00.4秒	10.2	52.2	1.4	0.0	124
過熱保護	4分09.4秒	7.6	80.2	1.4	0.0	139
停止	4分09.7秒	9.9	79.9	0.0	0.0	149

5. 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信頼性向上のため，FTA に基づいたログデータ収集機構について提案した．本手法は，障害発生時点の発生時刻や発生箇所などの基本的なログデータに加えて障害に関連する詳細なログデータも収集できる．

実験例の結果から，ログデータの収集に伴うオーバーヘッドはあらかじめ見積もることができ，制御タスクに比べて小さく抑えることができることが分かった．

参考文献

[1] 水野忠則　他：組込みシステム，　pp. 52-65 および pp. 136-149，共立出版，2013.

[2] デンソー カーエレクトロニクス研究会，“図解カーエレクトロニクス［下］要素技術 編”，日経 BP 社，pp. 209-213，2010.

[3] Nancy G. Leveson: Safeware System Safety and Computers，翔泳社，pp. 305-313，2009.

[4] 福岡省吾 他：リアルタイム制御システム用のログデータ収集スケジューリング，情報処理学会全国大会講演論文集，Vol. 76，No. 1，pp. 59-60，2014.

[5] μITRON(SH2) 組込み学習キット KED-SH101，共栄エレクトロニクス，技術解説書，2007.

[6] RoboCar1/10 for Automotive Platform, http://www.zmp.co.jp/products/robocar-110_package_option#ap（2016 年 1 月 26 日参照）.

[7] 北川裕貴　他：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，pp. 158-164，2014.