1J-4

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

福岡省吾† 山下昭裕†† 水野忠則† 中條直也†
† 愛知工業大学 情報科学部
†† 三菱電機エンジニアリング（株）

1. はじめに

近年，医療機器や自動車に代表されるリアルタイム制御システムが多数開発されている．こうした医療機器や自動車では人命が関わることがあるため，非常に高い信頼性が求められている[1]．

信頼性向上の手段として，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．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]．

しかしこうした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について提案する．障害箇所と収集するログデータを特定する手法として，フォールトツリー解析[3]（以下FTA: Fault Tree Analysis）を参考にしている．

2. 関連研究

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がある[2]．

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を記録する．また，車両の状態データも記録する．この障害発生を検出した時の状態データをフリーズフレームデータ(以下 FFD)という．

しかし，FFD は基本的な状態データしか収集できない．障害コードと FFD では障害に関する情報が少なく，システムが複雑になると障害原因の診断が困難になる．そこで，障害原因の診断には発生する障害に合ったログデータを数多く収集することが求められる．

3. モジュール関係に基づくログデータ収集

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(図 1)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ような機構である．こうすることで，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ことができる．

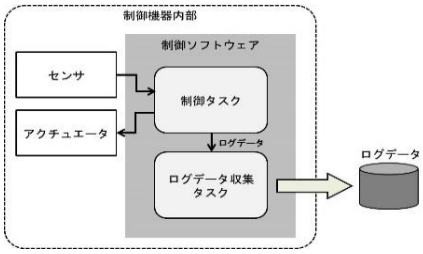

図 1: 提案するログデータ収集機構

Scheduling for Logging of Realtime Control Systems
Shogo Fukuoka†, Akihiro Yamashita††, Tadanori Mizuno†, Naoya Chujo†
† Faculty of Information Science, Aichi Institute of Technology
†† Mitsubishi Electric Engineering Co., Ltd.

3.2 障害箇所と収集するログデータの特定

提案するログデータ収集を実現するには，障害に対して事前に収集するログデータを決定しておく必要がある．そこでFTA[3]を参考に，発生する障害に対して障害箇所と収集するログデータをフォールトツリー(以下 FT: Fault Tree)[3]を用いて特定しておく[4]．

また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，モジュール毎のログデータを収集する．さらに，それぞれのモジュールで収集するログデータを静的に決定する．障害発生時には FT で決まるログデータのアドレス参照のための時間がオーバヘッドとなる．このアドレス参照の時間を含め見積もりを行った上でログデータ収集のスケジューリングを行う．

3.3 想定する障害事例と FT 展開例

ここで想定するモジュールの構成と障害の事例を考える．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，サーボアンプと通信して制御している．本研究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た．

障害の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したことを想定する．また，制御ソフトウェアの通信部分のモジュール構成を図 2 のように想定する．

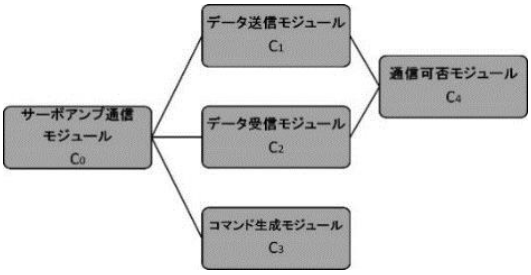

図 2: 通信部分のモジュール構成

図 3 は，サーボアンプとの通信障害についてあらかじめ原因となる事象を列挙した FT である．図 3 の色分けされているところが通信障害に関連する箇所，および原因である．図 3 の FT 展開に，モジュールを割り当てたものが図 4 である．本手法では，図 4 に示す 3 つのモジュールのログデータを収集する．

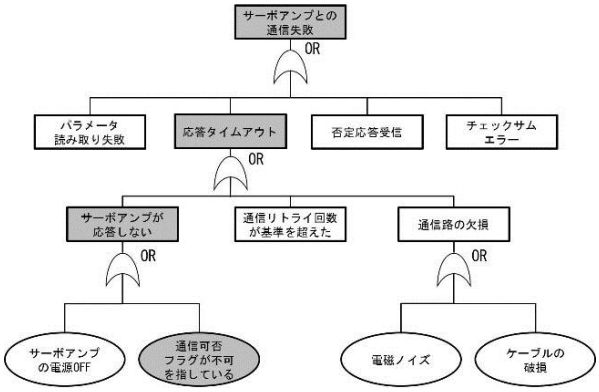

図 3: 通信障害における FT 展開図

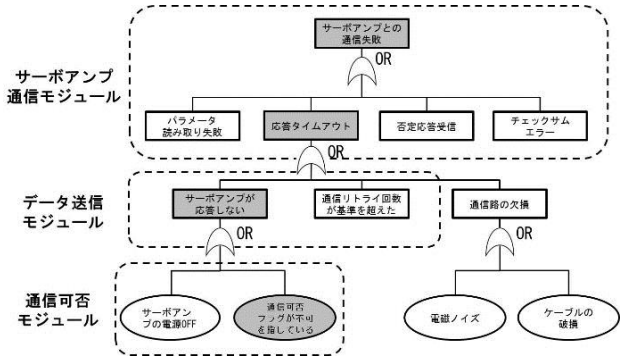

図4: 通信障害の原因があるモジュール群

4. 実験

4.1 実験方法

提案手法を定量的に評価するための実験を行った．ここでは通信障害における事例を取り上げて，リアルタイムで制御する通信システムを実装した．

実験には図5のような2つの組込みボードを用いた．このボード同士をRS-232Cを用いて通信させ，モニタするコンピュータからデータを計測した．

障害の事例は3章で取り上げたデータ送信時にタイムアウトする事例を再現した．

また，対象となるデータ送信制御タスクの基本実行周期は25msecである．

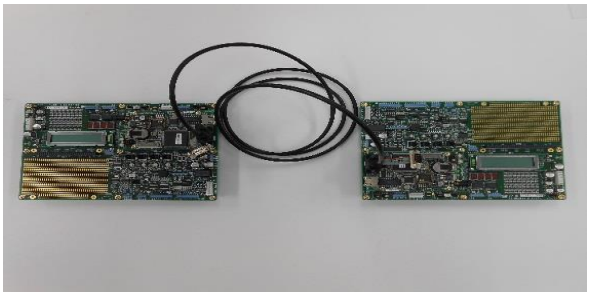

図5: 実験に使用した機材

4.2 実験結果

表1は収集したログデータのバイト数と内訳である．モジュール名は障害を検出したモジュールで，図4のサーボアンプ通信モジュールに相当する．

表2は障害発生時にログデータ収集にかかった時間と，障害発生後に一定周期の間で収集し続ける時の1周期でかかった収集時間である．また，収集したログデータの1バイトあたりの収集時間も算出した．

ログデータ収集タスクでは障害発生時の収集時間は39byteのログデータで7msecであった．これはログデータの存在するメモリアドレスを参照することで時間がかかっていた．

この例ではFT内データのメモリアドレス参照の時間も含めて，障害発生時のログデータ収集には1バイトあたり0.18msec必要であった．この値を使用してログデータ収集の周期を見積もることができる．

表1: 収集したログデータのバイト数

現状の収集バイト数合計	39	byte
モジュール名	9	byte
エラーコード	4	byte
レジスタ値	1	byte
送信データ	17	byte
リトライ数	4	byte
記録時刻	4	byte

表2: 1バイトあたりの収集時間

収集ログデータバイト数	39	byte
収集時間平均(周期データ)	1	msec
収集時間平均(障害時データ)	7	msec

1バイトあたりの時間		
周期データ	0.026	msec
障害時データ	0.18	msec

なお，その後も同じログデータを記録する際には，メモリアドレス参照を終えていることから，収集時間は1msecであった．

この場合，周期データの1バイトあたりの収集時間は0.026msecであった．

実験例では，データ送信制御タスクの実行周期時間の25msecと比較して，ログデータ収集タスクの障害発生時には7msec，周期データ収集時には1msecと十分に小さいことがわかった．

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，モジュール関係に基づいたログデータ収集機構について提案した．

ソフトウェアを構成するモジュールを基準として，障害発生時に障害箇所となるモジュールを特定し，ログデータを収集する手法を示した．

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，ログデータ収集タスクの実行周期はFT内データのメモリアドレス参照によって制約されることがわかった．これに基づいてログデータ収集のスケジューリングを行う必要がある．

今後は様々なリアルタイム制御機器に対して本手法を適用し，検証を行っていく必要がある．

参考文献

[1] JIS-Z8115:2000 “デイペンダビリティ（信頼性）用語 Glossary of terms used in dependability”.
[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] 高橋正和, “組込みソフトウェア向けの故障木解析手法”, 情報処理学会研究報告, Vol. 2013-SE-182 No. 24, 2013.