2008－EVA－24 (3)
2008／3／19

系再構成機能を適用した分散制御システムに関する一検討

望月 寛　　高橋 聖　　中村 英夫

日本大学理工学部電子情報工学科

近年、リアルタイムでのより高度な作業を実現するために、複数のコントローラを用いた分散制御システムが注目されており、このようなシステムの高信頼化へのニーズも高まってきている。それに対し、筆者らは、故障時にその他のコントローラの計算資源余裕を利用し、機能を代行する「系再構成機能を持つシステム」の概念を分散制御システムへ適用した。これにより、従来のように予備系を用いることなくシステムの高信頼化を図ることが可能となり、コスト削減などの効果が期待できる。そして、実際に複数のマイコンからなる分散制御システムを構築し、系再構成機能の実装を行った。さらに、使用するコントローラのハードウェア資源やシステムの要求性能を考慮して、汎用的な系再構成機能を適用した分散制御システムの構成を示し、その信頼性についても考察したので、あわせて報告する。

A Study on Reconfiguration Method in Distributed Control System

Hiroshi MOCHIZUKI, Sei TAKAHASHI, and Hideo NAKAMURA

Department of Electronics & Computer Science, College of Science & Technology
Nihon University

At present, distributed control system that realizes more advanced work in real time is noted. This time, to distributed control system, we applied reconfiguration method which inherits functions using calculation resource margin of other PCs. As a result, we realized improvement of reliability without using standby PCs. And we verified proposal method using distributed control system that configured by some microcomputers and sensors. In addition, we studied composition of reconfiguration method considered improvement of real-time processing that is one of benefits of distributed control.

1 はじめに

近年のネットワーク技術の進歩により社会システムの増大に加え巨大化、複雑化が進み高信頼化のニーズが増大している。システムに依存する世の中において、システムに障害が発生した場合、多くの人命が失われたり、莫大な経済的損失を受ける可能性は高く、現代の信頼性という分野の役割はとても大きい。

例えば、様々な産業分野において、その機器に対してリアルタイムでのより高度な作業が要求されている。その実現手法として、複数のコントローラを用いた分散制御システムが注目されており、現在、様々な研究開発が行われている。

ここで、このようなシステムの信頼性を向上させるための一般的な戦略としては、システムを構成する系を冗長化することがあげられる。しかし、システムの冗長化は信頼度を向上させる一方で、コスト増加の問題を生じる。また、設置面積も増大することになる。

これに対して、山本氏はあらゆる系に置換可能な2台の処理部を共通予備として持つことにより、各処理部に予備系を持つ単純な高信頼化手法に比して、大幅なハードウェア量削減を達成しつつ信頼度向上が可能となることを明らかにしている [1][2]。

本研究では、これらの検討を踏まえた上で、予備系を全く用いず、故障時にその他のコントローラの計算資源余裕を利用し、機能を代行する系再構成機能による高信頼化手法を提案し、実際の分散制御システムへ適用を試みた [3][4]。そして今回、系再構成機能を有する分散制御システムの一例として、実際にマイコンカーを製作し、マイコンの入出力ピンや各種ハードウェア資源を考慮したリリーフ機能を提案、検討を行った。

さらに、分散制御システムの採用のメリットが、リアルタイムでの処理性能の向上であることに配慮し、これを損なわない系再構成機能の適用手法を検討し、その信頼性も含めて考察した。

2 系再構成機能

2.1 概要

故障系の処理を引き継ぐ系をリリーフ系と呼ぶ。一般に処理部の負荷は高いものであるとすると、一台の処理系で機能リリーフが行えるとは限らない。そこで、故障系のタスクをいくつのリリーフ系に代行させるかを表現するために粒度 (particle size : P) という尺度を用いる。図1にその概念図を示すが、このようにm台の処理部に分割しリリーフさせた場合の粒度は、1／mと定義する。

また、リリーフ系は代替機能のソフトウェア資源を予め用意しておくばかりでなく、処理をスムーズに代行するための引き継ぎデータを一定時間ごとに登録しておく必要がある。故障系が発生した場合には、故障系を同定し登録したデータを用いて機能を代行する。

以上の観点から、次に示す2つのモデルを提案する。

2.1.1 サーバクライアントモデル

図2にサーバクライアントモデルを示す。この図によると、各処理部の機能をサーバが管理し、リリーフを想定して処理履歴を各系から収集し準備する。故障発生時には、サーバが故障系の同定を行い残りの系に対して機能のリリーフを指示する。

2.1.2 マルチマスタモデル

図3にマルチマスタモデルを示す。この図によると、予め各処理部が他系の機能の一部または全てを有する。そして、相互に交換する故障診断データにより、異常な処理部が検出された時には、その処理部に代わり残りの系が故障処理部をリリーフするような構成となっている。

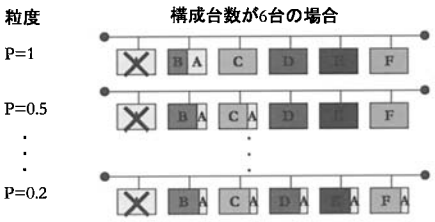

図 1: 粒度の概念図

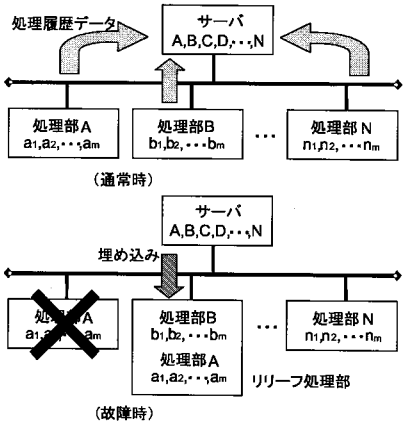

図 2: サーバクライアントモデル

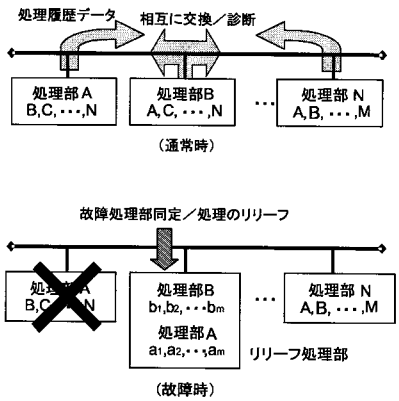

図 3: マルチマスタモデル

2.2 評価

前に述べた 2 つのモデルに対して、それらの性能を比較し、評価する。今、故障率 $\lambda = 20FIT(20 \times 10^{-9})$ を持つ 6 台の処理部によって構成されるシステムを仮定し、提案する両モデルの不信頼度評価を行なった結果を図 4 に示す。ここで、サーバ 1 台の故障率は同様に λ であるが、システム全体の信頼度強調のため冗長構成を図り、λ^2 となっているものとする。先に述べた粒度を大きくすれば、両モデルにおいて全ての系に予備を持つ待機冗長方式に比しても信頼度の向上が見られる。また、粒度が 0.33 以下ではいずれも、待機冗長

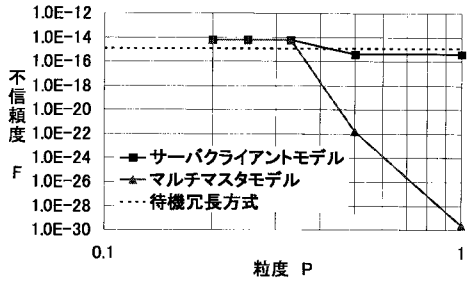

図 4: システムの不信頼度評価

方式より信頼度は悪くなるが、これらはほとんど冗長性を含まない状態での信頼度改善といえ、系再構成機能の有効性を否定するものではない。

3 系再構成機能の分散制御システムへの適用

3.1 複数のマイコンを用いた分散制御システムの特徴

前節で系再構成機能を有するシステムの概要について示したが、ここでは実際のシステム、特に分散制御システムへの適用について検討する。

今日、我々の身の回りのさまざまな製品にマイコンが内蔵されており、特に、複数のマイコンを有し、各マイコンに異なる機能を与え、それらの連携動作により、リアルタイムでのより高度な作業を実現する分散制御の構成をとるシステムも多くなってきている。このような分散制御システムにおいて、故障に備えて各マイコンに冗長系を付加した構成は、コストやハードウェアの増大につながる。

他方、分散制御システムに用いられている各マイコンに関しては、それが持つ一部の I/O ピン及びハードウェア資源のみを用いて構成していることが多く、計算資源には余裕があると考えられる。さらに、連携動作を行うためにマイコン間には通信路が確保されているという特徴も有している。

以上の点を考慮して、前節で示したマルチマスタモデルを、複数のマイコンを用いた分散制御システムに適用する。具体的には、リリーフ時に備え各マイコンには、通常時に自身が担当する機能以外の一部または全ての機能を実現するためのソフトウェアをあらかじめ実装しておく。さらに、従来、制御情報のやりとりを行うマイコン間の通信路を用いて、以下に示すような手法により故障診断及びリリーフを行う。

1. マイコン間で、故障検知のためにハートビートメッセージのやりとりを行う。ここでのハートビートメッセージのやりとりには、ハートビートメッセージ (ASK) が送られてきたらハートビートメッセージ (ACK) を返して自分の生存を知らせるプル型方式を採用する。

2. ASK を発信したコントローラは一定時間内に ACK がなければ受信側のコントローラが故障していると判断する。

3. ASK を受信したコントローラは、ただちに ACK を送信し、一定時間後に ASK を次のコントローラに対して発信する。

4. 故障を検知したコントローラはシステム内に故障を伝達し、正常なコントローラが機能をリリーフする。

なお、実際のリリーフに関しては、各マイコンの機能は大きく分けると入力と出力との 2 つであることより、故障時においては、それら両方を 1 つのマイコンでリリーフする粒度 1 の場合と、それらを別々のマイコンでリリーフする粒度 0.5 の場合とが考えられる。

3.2 マイコンカーへの実装

ここまでの検討を踏まえて、分散制御システムの一例として、実際にマイコンカーを製作し、マイコンの入出力ピンや各種ハードウェア資源、及びリアルタイム性を考慮し、系再構成機能の概念を適用した。

今回、ターゲットシステムとして製作したマイコンカーのブロック図を図 5 に、外観を図 6 に示す。図 5 に示すように、このマイコンカーは超音波センサ、赤外線受光モジュール、フォトインタラプタの 3 つのセンサを有し、各処理部にコントローラとして独立のマイコンを搭載している。

以下に、各センサの働きなど、マイコンカーの概要を示す。

1. 3 つのセンサとそれぞれのマイコンを持ち、軌道上を走行する。軌道上の障害物を検知して停止する他、速度制御が可能である。

2. フォトインタラプタは、黒い線上を走行するためのセンサであり、左右のモーターへの出力を制御する。

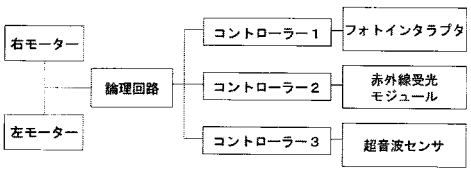

図 5: マイコンカーのブロック図

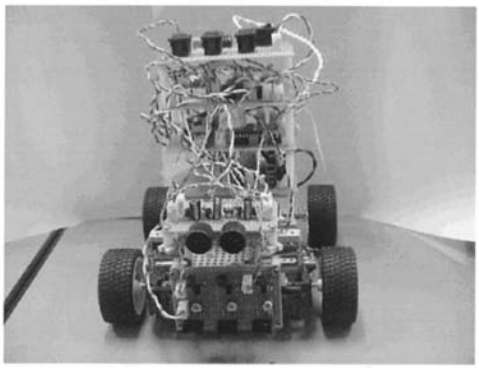

図 6: マイコンカーの外観

3. 超音波センサは、軌道上の障害物を検知し、障害物がある場合にはマイコンカーを停止させる。

4. 赤外線受光モジュールは、コース外に設置された赤外線 LED からの信号を受信し、指定された速度で走行するようにモーターへの出力を制御する。

各コントローラには PIC (Peripheral Interface Controller) を採用した。今回使用した PIC16F876 では 22 の I/O ピンを有する他、5 つの A/D コンバータ、3 つのタイマ、さらに 2 つの CCP(キャプチャ/コンペア/PWM) モジュールなどを有する。表 1 に今回のマイコンカーで使用したハードウェア資源をまとめたものを示す。

表 1: マイコンカーで使用したハードウェア資源

名前	搭載数	フォト	赤外線	超音波	診断
I/O	22	7	2	2	7
A/D	5	0	0	0	0
タイマ	3	0	1	1	0
CCP	2	0	1	1	0

ここで、表 1 中、フォトインタラプタによるライントレースにおいては、今回、3 つのセンサを用いて左右のモータ制御を行っているため、I/O ピン数を 7 とした。また、故障診断においては、故障診断データの他に、現在の各マイコンでの処理状況などをやり取りすることも視野に入れて、同様に I/O ピン数を 7 とした。その他のモジュールに関しては、入力と出力を 1 ピンずつ割り当てた。また、超音波センサでは、センサ出力を一定サンプリングでマイコンに入力するため、さらに、赤外線受光モジュールでは、速度制御を行う際に、PWM 制御を行うために、タイマと CCP モジュールをそれぞれ 1 つずつ割り当てることとした。なお、今回のマイコンカーにおいては、A/D コンバータは使用しなかった。

以上、各モジュールに対する具体的なハードウェア資源割り当てについて示したが、全てのモジュールに割り当てられたハードウェアの総数は、表 1 に示した PIC16F876 の搭載数内に収まっており、今回のマイコンカーに関しては、各マイコンに全てのモジュールをあらかじめ実装しておくことが可能となる。また、ハードウェア資源余裕がなく、各マイコンに全てのモジュールを実装できない場合においても、故障マイコンとリリーフ用マイコンとの対応テーブルを作成するなどの配慮により、系再構成機能が適用可能であると考えられる。

これらのことを踏まえて、今回製作したマイコンカーに関して性能評価を行った。具体的には、あるマイコンに電源を投入せず、故意に動作しない状態となるような模擬故障を与えた場合に関して、ハートビートメッセージによる故障検知、及びリリーフ性能を評価した。その結果、正しく故障検知が行われ、かつ、他のマイコンへのリリーフが正しく行えることを確認し、系再構成機能の有効性を実証できた。

4 サーバクライアントモデルの適用に関する考察

前節で、今回のターゲットシステムである分散制御システムに対して、マルチマスタモデルによる系再構成機能を適用し、その性能を確認した。

しかし一方で、分散制御システムで複数のマイコンを用いて機能分散をする理由の 1 つとして、リアルタイム性の実現など処理速度の向上を図ることが挙げられる。ここで、マルチマスタモデルによる系再構成機能を適用するということは、各マイコンにハートビートメッセージなど他のマイコンのヘルスチェックや機能代行を決定する処理を加えなければならず、その結果、処理速度の低下、さらにはリアルタイム性を確保できなくなる可能性が生じる。そ

こで、筆者らは、サーバクライアントモデルによる系再構成機能により、前述の問題点を解決を試みた。

今回、ターゲットマイコンとしてH8/3048Fを例に挙げると、これは下記に示すようなハードウェア資源を有している。

- 最大動作周波数：16MHz
- ROM：128kバイト
- RAM：4kバイト
- 割り込みコントローラ
  - 外部割り込み端子7本
  - 内部割り込み30要因
- DMAコントローラ（DMAC）
- タイマユニット（ITU）：16ビットタイマ5チャネル内蔵
- ウォッチドッグタイマ（WDT）：1チャネル
- シリアルコミュニケーションインタフェース（SCI）：2チャネル
- A/D変換器：10ビット8チャネル
- D/A変換器：8ビット2チャネル
- I/Oピン：入出力端子70本入力端子8本

ターゲットシステムにもよるが、一般的に、I/Oピンなどのハードウェア資源が余る場合が多い点に着目し、図7のような構成を提案する。

図7のように、制御用マイコン間でハートビートメッセージなどの通信を行わず、制御用マイコンでは、余剰のI/Oピンに各種ハードウェア資源を制御するレジスタ情報の出力のみを行い、それを故障診断用マイコンが収集する形を取る。故障診断に関しては、これらの情報が得られなくなった場合に故障と判断し、他のマイコンへと機能を代行する。また、各制御用マイコンとモータ・センサとのインターフェースにI/Oボードを使用し、故障診断用マイコンの制御信号によって、接続を動的に変化できるようにする。

また、図7において、故障診断用マイコン自体の故障が懸念される。しかし、これは制御用マイコンの監視のみの機能を有しており、センサ・モータなどの駆動系とは独立している。したがって、制御用マイコンのウォッチドッグタイマなどを使用し、一定時間以上、故障診断用マイコンの通信がなかった場合に故障と判断し、それに基づいた修復によって機能を継続させる。

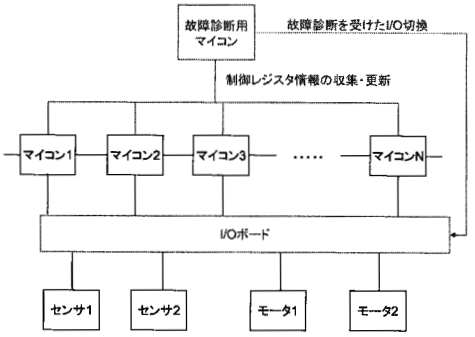

図7: サーバクライアントモデルによる系再構成機能

以上、提案した構成で制御用マイコンに故障診断機能を持たせないことにより、従来の処理速度の低下を防ぎつつ、系再構成機能を適用することが可能である。

5 まとめ

本稿では、システムの信頼性を向上させる手法として、コスト面や設置面積の増大などに配慮し、予備系を全く用いず、故障時にその他のコントローラの計算資源余裕を利用し、機能を代行する系再構成機能を提案した。その構成としては、サーバクライアントモデルおよびマルチマスタシステムを取り上げたが、評価の結果、いずれの手法においても待機冗長系に比して、信頼度の向上が図れることを確認した。

以上の成果を踏まえて、複数のコントローラを用いた分散制御システムをターゲットシステムとして、実際に製作したマイコンカーにおいて、任意のマイコンの故障に対して、マルチマスタモデルによる系再構成機能の概念を適用し、システム内に故障を伝達することによってフォールトトレランスを実現した。

さらに、サーバクライアントモデルにより系再構成機能の適用可能性についても考察し、モータ・センサを制御するマイコンの他に、故障診断用マイコンを付加し、それが各マイコンの制御レジスタの情報収集や書換を行うことにより、処理速度を低下させることなく系再構成機能を適用できる見通しを得た。

今後の課題として、マルチマスタモデルについては、マイコン数が多くなった場合のネットワーク構成や機能代行の手順の確立、また、サーバクライアントシステムについては、今回の提案手法を実際のシステムに実装した上で評価、及びI/Oボードの高信頼化について検討し、更なる研究の深度化を図っていきたい。

参考文献

[1] 山本正宣「資源共有化によるATCシステムの高信頼化とその評価」電学論D vol.123 no.5 pp.612-622(2003).

[2] M. Yamamoto, S. Takahashi and H. Nakamura, "Dependability Verification of Architecure changed Automatic Train Control Sustem" ISIE in IEEE pp.417-422(2001).

[3] 志賀一之、望月寛、高橋聖、中村英夫、「フレキシブルな系再構成機能を持つシステムに関する一検討」、第13回春季信頼性シンポジウム発表報文集 4-3(2005).

[4] 志賀一之、望月寛、高橋聖、中村英夫、「系再構成機能を持つシステムの応用」、電子情報通信学会技術研究報告 DC2005-67(2005).