技術紹介

耐障害性向上を目的とした通信ミドルウェアの開発

～タイムトリガ方式による分散制御システム～

Development of Fault Tolerant Communication Middleware

金平　徳之
Noriyuki KANEHIRA
川田工業㈱機械システム事業部
ロボティックス部課長代理

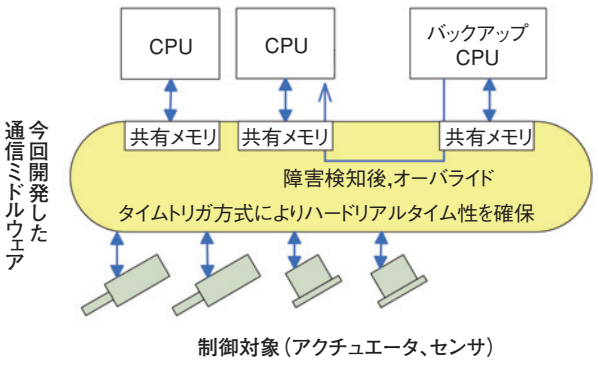
宮森　剛
Go MIYAMORI
川田工業㈱機械システム事業部
ロボティックス部係長

自律移動体は，無人で移動し，与えられたミッションを達成することを目的とするロボットシステムです。例えば（独）海洋研究開発機構の保有するうらしまやMRX-1[1]は長時間無人で海底を探査し，情報を収集して持ち帰る目的で開発されたロボット潜水艇です。このようなロボットシステムに対しては，信頼性の確保が大きな課題の一つとなります。例えばミッションの途中で機器の故障やシステムの障害が発生すると，ミッションの遂行が不可能になるばかりでなく，ロボット自体の回収を行うことができなくなり，多大な損失を招くことになります。そこで当事業部では，信頼性のある自律移動体制御システムの確立を目指し，汎用的な，耐障害性を有する通信ミドルウェアを開発しました。本稿では，この通信システムの基本概念と技術的特徴について説明します。

本システムの基本概念

信頼性を確保する方法としては，
①個々の部品の信頼性を保証する
②システム全体としての信頼性を保証する
の2通りが考えられます。

このうち，①については，市販品として利用できる部品の仕様に限界があることや，故障回復処理時のシステム整合性の煩雑さなどの問題があり，結果としてコスト増加を招く場合があります。そこで，われわれは②のアプローチを採用し，複数のCPUを用いて相互に監視し合う方法をとることにしました。次図がそのシステムの概念図です。各CPUは共有メモリに書き込まれる他のCPUやセンサノードの情報を読み取り，それぞれのCPUに割り当てられた計算を行い，計算結果を共有メモリに書き込みます。CPUの故障が検知されると，バックアップCPUが故障したCPUの役割をオーバライドし，ミッション継続或いは非常動作の処理を行います。なお，バックアップするCPUは専用のバックアップCPUである必要はなく，計算能力に余力があれば，他のCPUにバックアップの処理を行わせることも可能です。



システムの概念図

システムの特徴

本システムの特徴は，
・タイムトリガ[2]を用いた通信プロトコル
・多重系CPUによる相互監視・補間機能
・通信経路の2重化
・ミラーリング[3]によるメモリの共有化
であり，いずれについても新規にソフトウェアを開発しました。以下に詳細を説明します。

（a）タイムトリガを用いた通信プロトコル

通信プロトコルのベースとしてはCAN[4]を用いました。CANは自動車の車内制御用通信プロトコルとして標準的に用いられており，CANが実装されたCPUチップやCPUボードは容易に手に入れることができます。CAN自身も耐障害性の機能を持っていますが，基本的にイベントトリガ式であるため，通信量が多いときにはメッセージの遅延が頻繁に生じることになります。故障検知のタイミングが重要になってくる移動体へのアプリケーションの場合，この遅延は致命的になるときがあります。そこで，CAN上にタイムトリガと呼ばれる通信方式を独

自に構築し，定められたタイムテーブルに従って通信を行う仕組みを設けました。これによりメッセージの厳格なスケジューリングが可能となり，故障の早期検知が可能となりました。

（b）多重系CPUによる相互監視・補間機能

CPUの障害は他のCPUによって監視されます。一旦障害が検知されると，正常なCPUが故障したCPUのタスクをオーバライドできるような補間機能を設けました。なお，正常なCPUによる補間機能については，データの整合性や障害発生後の回復処理のシーケンスが，本システムを実装する自律移動体全体のシステムによって異なるため，今回の開発では完全な補間機能まで作りこむにいたってはいません。

（c）通信経路の2重化

通信システムの耐障害性を増すため，2重の通信経路を設けました。具体的には各CPU間をつなぐCANモジュールを2つずつ用意し，それぞれを独立した配線でつなぐこととしました。これにより一方の通信線の断線や通信モジュールの故障が発生しても，もう一方の通信線でオーバライドすることができ，通信網の信頼性を上げることができました。

（d）ミラーリングによるメモリの共有化

CPUが故障した場合，そのCPUが持っていた情報をバックアップCPUが引き継ぐ必要があります。そのためにはメモリの情報をCPU間でリアルタイムに共有する必要があります。これを実現するため，CANバス上に流れるデータを全てのCPUがそれぞれの持つメモリにリアルタイムで書き込む方式を取ることにしました。

実際のシステム

（a）ハードウェア

制御用CPUボードとしては，アルファプロジェクト社のMS104-SH4を用いました。このCPUは汎用的なPC104バスを有しており，さまざまな機能を持つ拡張用ボードを市販品で手に入れることができます。CAN通信用のボードには，Gridconnect社製のGC-CAN-PC104-2を用いました。下表にこれらのボードの主な諸元を示します。

主なハードウェアの諸元

項目		名称
CPUボード： アルファプロジェクト製 MS104-SH4	CPU	SH7750R (MS104-SH4)
	クロック	235.9296 MHz (19.6608 MHz水晶振動子)
	SDRAM	64 MB
	拡張バス	PC/104バス配列準拠
CAN通信ボード： Gridconnect社製 GC-CAN-PC104-2	通信速度	1M bps
	チャンネル数	2

（b）OS

OSとしては，Linux kernel 2.6[5]を採用しました。Linuxは kernel 2.6になってプリエンプション機能が標準的に使用できるようになりました。これによりタスク起床レイテンシが改善され，ソフトリアルタイム性を獲得しています。

下記に今回開発したシステムの外観を示します。

開発したシステムの外観

システム実装結果

開発したシステムにアクチュエータやセンサのデバイスを接続し，通信システムを作動させました。そして，スケジューリング上での通信，障害検知などをテストし，システムの正常な動作を確認することができました。

まとめ

耐障害性を目的とした多重CPUによる分散制御システムの通信ミドルウェアを開発し，その基本機能のテストまで行いました。課題として，バックアップCPUによるオーバライドの具体的なシーケンスの構築や耐久試験などが残っています。今後は，本システムを具体的な自律移動体に組み込み，問題点を改善し，有効性を確認していく予定です。

なお本報告は（独）海洋研究開発機構との共同で行った開発の一部をまとめたものです。

参考文献

1）http://www.jamstec.go.jp/jamstec-j/maritec/amtp/autonomous/index.html

2）B. Muller, T. Fuhrer, F. Hartwich, R. Hugel, H. Weiler, Robert Bosch GmbHHill, Fault tolerant TTCAN networks, http://www.canopen.org/can/ttcan/mueller.pdf.

3）佐藤道夫：車載ネットワーク・システム徹底解説，CQ出版社，2005.

4）当麻喜弘，南谷崇，藤原秀雄：フォールトトレラントシステムの構成と設計，槇書店，1991.

5）インターフェース７月号，CQ出版，2005.