解説

これからの通信技術

—通信安全の話題—

Oncoming Robot Communication Technology

—Communication for Safety-Related Systems—

山田 陽 滋^{*1} 中 坊 嘉 宏^{*1} 齋 藤 元^{*2} ^{*1}産業技術総合研究所 ^{*2}ゼネラルロボティクス (株)

Yoji Yamada^{*1}, Yoshihiro Nakabo^{*1} and Hajime Saito^{*2} ^{*1}AIST ^{*2}General Robotix, Inc.

1. はじめに

ロボット安全の観点 [1] におけるロボット通信技術に関する主な関心は、

- 通常の通信技術と、安全に配慮した通信技術と何が異なるのか？
- ますます高い情報処理能力の要求されるロボット分野にとって、どのような通信技術の導入が望まれるか？

であろう。

前者は、適切な通信規格を参照することによって、また後者は、当該分野最新のネットワーク通信技術を紹介することによって、それぞれ把握することができる。以下まずは、ロボット通信の最近の話題から導入を試み、通信の安全規格を紹介することにする。

2. ロボットの安全制御と通信

2.1 ロボット通信の安全化とは

ロボット分野において、人がロボットと触れないことを安全確保の基本とする、産業環境におけるロボットを対象とした安全規格においても、作業エリアの中でペンダント制御装置から無線によるロボットの保護停止を行ってもよい、と最新の規格改定では認められるようになった [2]。この無線による停止機能については、電線を引きずり回さずに教示作業等ができることから、現場の歓迎する技術として日本のみならずその規格化には支持が集まった。保護停止とは、再起動を容易にするために、プログラム論理を保持して、つまり制御装置の電源は供給したままで、ドライバ側の電源だけ遮断すればよいとする停止のさせ方である。産業環境におけるロボットの場合、アクチュエータの停止の方法については電源の供給を寸断するか、あるいは停止

過程においてのみ電源供給を維持しながらロボットを停止させ、停止したら電源を遮断する、という停止のさせ方までが許される。

つまり、安全に配慮した通信規格は、通信性能そのものを規定するというより、その性能が劣化した場合あるいは通信機能が維持できなくなった場合に、安全関連系と呼ばれる一連のシステムが安全な状態に至るようなメカニズムとしてできあがっているかを規定するところに特徴がある。ここで、安全関連系とは、機械安全の分野では、機器の制御装置に異常事態が発生した場合に、機器を安全な状態に移行する、あるいは安全状態を保持するために必要な安全機能を実行することを目的として、通常の制御系とは独立に設けられるシステムのことである。

2.2 無線制御

本章冒頭で導入した話題を関連規格の紹介で結んでおくことにしよう。安全関連系で制御停止 (controlled stop) の信号のみは、ある条件を満たせば、有線のみならず無線で伝送してもよいことが国際安全規格としてすでに成立している。すなわち、機械の電気機器 [3] を対象としたグループ規格では、制御回路および制御機能に関する安全要求事項の中で、オペレータ側の制御ステーションと機器側の制御システムとの間のコマンドや信号の無線通信を、

- 機器や危害を加えるおそれのある運転を停止する個別の制御手法をもっていること
- しかし、この停止機能の発信手段は、緊急停止装置と位置づけてはならないこと

という条件下で認めている。また、無線による制御機能を備えた機器は、

- 停止信号が受信された場合
- 無線制御システムの中で不具合が検出された場合
- あらかじめ宣言された通信周期の間に有効な信号が検出されなかった場合

に、自動的に停止機能が起動するようになっていなければならない、とおおよそ自明の規定がある。

次章では、ロボットの場合のみならず、より一般の機械制御システムに適用可能な通信安全規格の概説を行う。

原稿受付 2008 年 1 月 15 日

キーワード: Safety Communication, Safety-related System, Safety Standard, Functional Safety, TTP/C

^{*1}〒 305-8568 つくば市梅園 1-1-1

^{*2}〒 305-0047 つくば市千現 2-1-6

^{*1}Tsukuba-shi, Ibaraki

^{*2}Tsukuba-shi, Ibaraki

3. 通信に関する安全規格

3.1 機能安全

近年、機能安全[4]の概念が注目されている。これはソフトウェアを含む電子機器の機能により、安全性を確保するための規格であり、リスクアセスメント結果に基づいて設計者が定めるSIL (Safety Integrity Level) を基準に、安全妥当性を検証するプロセスを規定しているのが特徴である。SILはシステムが持つべき安全性能の水準を1~4のレベルに分けて示すもので、安全関連のハードウェアシステムにおいては、主に作動要求時の機能失敗確率、あるいは単位時間当たりの危険側故障率によって検証されるものである。

データ通信については、この機能安全に関する概念規格の中に記述の項目があり、通信で安全に関わる考慮すべき点を短く示した上で、詳細については鉄道分野における通信・信号処理の安全規格EN50159-1, 2[5]ほかを参照することとしている[4]。以下では、この鉄道応用の通信安全規格について簡単に説明する。

3.2 鉄道通信安全規格

EN50159は、鉄道における安全関連の通信システムの構成方法に関するものであるが、内容は鉄道に特化せず、ロボットを含む一般の通信にも広く使えるものとなっている。国際規格のIEC62280-1, 2は、これとほぼ同じ内容である[5]。規格は大きく2部に分かれ、

- Part 1: クローズドな通信システム
- Part 2: オープンな通信システム

について書かれている。

3.3 クローズド通信システムの安全性

EN50159 Part 1では、クローズドな通信システムの条件として、

- (1) 通信ネットワークにアクセス可能な機器がすべて承認

済みのものであり、

- (2) 接続する機器の最大数が既知で、

- (3) 機器の特性が既知で固定されているもの

としている。これらの条件には、ロボットの内部ネットワークなどが該当すると言える。

通信システムの構造としては、専用の二重化通信系などではない、一般の任意のネットワークを想定している。これを信頼できない(non-trusted)通信システムとして考え、この上に独立したシステムとして安全関連の通信を行う安全関連通信システムを構築して、機能により安全性を確保するというアプローチをとっている。これを図1(a)に示す。また後述のオープン通信システムでも同様な構造を想定している。

具体的な安全対策としては、まずハザード分析から始めて、どのような誤りがシステムの危険を引き起こすか調べる。その際、通信内容の誤りに加え、時間的な遅れなどの影響も考慮する。さらにSILに基づいた危険側誤り率Rhを目標の安全性能とし、安全符号(safety code)を利用して安全性を確保する。安全符号の符号化、復号化などを行う安全関連部は通信系には依存せず、独立したシステムであることが重要である。また安全符号の長さは、信頼できない通信系での各種故障を考慮して決定する。具体的には、 $Rh = Rh1 + Rh2 + Rh3$ として、

Rh1 ハードウェア故障率: 通信系の故障を検知して安全動作が起動するまでの間の危険側故障率

Rh2 EMIに関わるランダム故障: 各種符号化にもかかわらず不良が発見できない確率

Rh3 通信用の符号器の不良でエラーが発生する場合の確率

としている。これらそれぞれの具体的な計算方法が、規格に例示されている。

図1 安全関連通信システムの対象

表 1 メッセージに対する脅威と、防護技術との対応

防護技術	メッセージに対する脅威						
	反復	欠損	挿入	誤配列	改変	遅延	偽装
シーケンス番号	●	●	●	●			
タイムスタンプ	●			●		●	
タイムアウト						●	
送受信者 ID			●				
メッセージフィードバック			●				●
同定確認手続			●				●
安全符号					●		
暗号					●		●

3.4 オープン通信システムの安全性

EN50159 Part 2 ではオープンな通信システムを扱う。未知性を持つあらゆる通信、メディアを対象としており、インターネット、外部機器を接続する LAN、無線などがこれに当たる。通信系はブラックボックスとして扱い、安全関連のメッセージに対する脅威 (threat) として、反復、欠損、挿入、誤配列、改変、遅延、偽装の七つを挙げている。またその対策として、シーケンス番号、タイムスタンプ、タイムアウト、送受信者識別 ID、メッセージフィードバック、同定確認手続、安全符号、暗号の八つを示している。それぞれの脅威に対する防護技術の対応関係については、表 1 のようなマトリックスが示されている。

このほかに、認証済み (authorized) アクセスだけを考えると、適用技術選択のポイントとしている。例えば LAN など許可されていないアクセスがあり得る場合には、暗号の使用が推奨されている。このようなシステムの外部条件と適用すべき安全技術の関係についても、具体的なチャートが規格の中で示されている。

3.5 文書化

前述の前提条件や考慮した脅威、適用した防護技術とその限界などについては、安全規定 (safety case) として明文化して保存し、必要に応じて利害関係者に提示することが求められている。これはシステムの開発段階から安全性について注意を払わなければならないという考え方に基づくものであり、ロボットの実用化を目標とした研究でも考慮すべき点であると言える。

4. セルレベル・ネットワーク向け安全通信技術

ここでは、ロボットのデータ容量の増大化にいかに対応するか？に答えるべく、近年注目を集めている高速安全バス TTP/C を紹介しよう。図 1(b) は、ロボットの基盤となる産業機械、あるいはプラントの制御を対象としたネットワークの体系を簡略的に示したものである。図 1 は、ネットワークのそれぞれのレイヤにおいて、処理される情報量

表 2 SAE 通信速度の分類

クラス	通信速度	用途
A	10Kbps 以下	車内環境を快適にする機器向け (オーディオ制御、トリップコンピュータ等)
B	10Kbps~125Kbps	一般的な情報機器向け (計器、車速センサ状態表示等)
C	125Kbps~1Mbps 以上	実時間制御向け (動力、車両の挙動制御等)
D	5Mbps~	マルチメディア向け (カーナビ、オーディオ等)

が異なることを示している。例えばフィールドレベルのネットワークでは、複数のセンサやアクチュエータの情報信号を一括して取り扱うことになるため、PLC などの導入が必要となる。ロボットは、その 1 台で、図の点線で囲んだセルレベル以下の範囲内のデータ処理を行う。ロボットは制御軸数が比較的多く、下位のフィールドレベルで組み込み系の導入によるドライバのインテリジェント化が進んだとしても、それらの信号情報を統合して制御に利用するとすると、やはりフィールドレベルと比べて時間当たり 10 倍程度の処理能力を要し、後出の表 2 に述べる「高速」レベルの通信速度が要求されることになるのである。以下に、TTP/C について概述する。

4.1 TTP/C について

TTP/C は Time Triggered Protocol Class C の略である。Time Triggered Protocol は時間幅をベースに定義されているプロトコルで、時間にあわせて必要なデータを通信する実時間制御向きの通信システムであり、Time Triggered Architecture (TTA) を採用している。TTA の特徴として次のようなことが上げられる。

- 定刻動作
- 階層化ではなく統合化
- 全ノードが相互通信スケジュールを把握
- 高いデータ送信効率
- シングルフォールト仮説に基づく通信状態管理機能
- 壊れても通信停止しない、ノードの通信システム飽和防止機能

Class C とは SAE (Society of Automotive Engineers) の通信速度のクラスで、車載 LAN では、通信速度を表 2 に示す四つのクラスに分類している。

表 2 から分かるように、TTP/A は低速なシステム用で TTP/C は高速なシステム向けのものとなっている。TTP 自体はオープンスペックな通信プロトコルであるため、誰でも仕様を入手することができる[†]。その結果、その信頼性の高さは形式検証等を用いて確認されている [6]。1998 年から通信チップや通信タイミングのセットアップをするためのツールが製品として存在しており、航空機や鉄道に使用されて実績をあげている。

[†]TTP の開発および販売を行っている TTTech 社に申し込む。

表 3 TTP で使用可能な物理相の比較

	RS485	光ファイバ	イーサネット
スループット	5Mbps	25Mbps	1Gbps
接続方式	スター/バス	スター	スター/ライン /ツリー

4.2 通信物理レイヤ

TTP は通信する間隔をベースとしている通信システムであるため、使用する物理層に対する制限はない。最初の TTP/C 通信チップは、物理層として RS485 を使用する非同期通信と、光通信を使用する同期通信の二つが使用可能であった。最近さらに TTEthernet が出てきており、これら三つのスループットと、可能な接続トポロジを比較すると表 3 のようになる。

システムが検知し得るエラーは接続方式により制限される。バス接続の場合はフェールセーフな動作が可能となるが、フェールオペレーショナルなシステムを構築したい場合はスター接続を選択することになる。これは、バス接続の場合には接続が切れてノードからの通信が不能になったのか、ノードそのものが通信タイミングを逃したのかを区別する方法がないからである。この結果、バス接続では、この状態を検知してフェールセーフにすることはできるが、ノードの通信タイミングがずれていることを検知してノードを再初期化するなど、フェールオペレーショナルなシステムとすることはできない。

4.3 タイム・トリガ・アーキテクチャの概要

TTA については、誌面の制限から大まかに説明するのみに留める。詳細な説明が必要であれば TTP の仕様を TT-Tech 社から入手するか、文献を参照されたい [8]~[11]。

このアーキテクチャは名前が示すように、定刻通りに通信するためのプロトコルである。これを満たすには全ノードで共通の時間を持ち、全システムが共通のスケジュールに従って動作する必要がある。

時間 TTA では、時間は過去から未来に一樣に進むものとしている。すべてのベースとなるのがグローバル時間である。通信チップには GPS と同様の時計と時間データを使用していて、最小時間刻みも GPS 同様 60[ns] である。システムで使用するグローバル時間の最小時間刻みは時計合わせ精度より大きくする。

状態 最小幅を持つ離散的な時間と状態とを組み合わせることによって、過去と現在とを区別することが可能になる。この離散的な時間により時間の把握を簡単化し、同じ時間に起きた現象は同時に起きたことにしている。

送信状態の管理 通信チップ内にはバスガーディアンと呼ばれるスイッチがあり、ノードの送信スケジュールにあわせて開閉する仕組みになっている。このため、送信状態でノードが固まったとしてもシステムを通信不

能にすることがない。耐障害性の高いシステムを構築する際、このバスガーディアンは独立に設ける必要がある。最近発表された TTEthernet は、このバスガーディアンをスイッチングハブに入れているのだと思われる。

時間割の共有 全ノードは他のノードが通信するタイミングをすべて把握している。この情報を使用してどのノードでも通信状態の確認が可能となっている。バスガーディアンは、この時間割にあわせ、ノードの通信線の接続・切断を制御している。

相互評価 時間割を共有しているので、他のノードの通信タイミングから正常に動作しているかどうかを評価することが可能である。この情報を使用して動作していないノードを見分け、バックアップノードを使用して動作を継続することも可能である。TTP/C ではノードに割り当てられている時間内に自分の通信データに加えて自分の前に通信した 3 ノードの通信内容の評価も同時に送信する。三つのノードに評価された結果、不良と判断された場合には、そのノードは通信メンバから外され、次の初期化フェーズまで通信に参加できなくなる。

冗長性 TTP コントローラはクラス C 通信が可能なポートを二つ持つ。両チャンネルで送受信するデータは自由で、同じであっても違って構わない。

耐障害性・単一障害仮説 TTP/C では次のような障害を想定していて、障害が起きてから十分な速度で障害の原因を特定することができれば障害に打ち勝てる (Never Give Up Strategy を持つ) システムの構築が可能となっている。

これら機能を組み合わせて、以下のような障害対策が施せるようになっている。

ノード内障害 ノード内で障害が起きた場合、バスガーディアンによりシステムはデータの送受信が不可能な状態に陥るのをまぬがれ、相互評価によってノードが使用不能になっていることを確認することができる。

ノード外障害 冗長な構成になっているノードであれば、単一ノードが使用不能になっても、システムとして動作し続けることが可能である。

コントローラ設計ミス ユーザの作成した通信スケジュールの確認はするが、コントローラそのものの設計ミスはないものと想定している。

ホストコンピュータソフトウェア設計ミス バスガーディアンがあるので通信障害を引き起こすことはないが、冗長性による利点がなくなることは考えられる。

仕様ずれによる通信障害 専用のバスガーディアンを設置することにより障害を回避することができるが、これ

はスター接続を使用した場合のみ可能である。

通信線の物理的な切断 冗長性を持たせることにより、ある程度の障害を回避することができるが、バス接続の場合には通信線が同じ場所を通っている可能性がある。そのため、このような障害に強いシステムを作成するにはスターもしくはリングトポロジを使用する必要がある。

5. お わ り に

本稿では、特に安全観点におけるロボット通信技術について述べた。まず、安全関連通信系について述べ、次に、セルレベルの情報処理速度に耐える実時間向きの通信システム TTP/C を取り上げ、その概要の解説を行った。

生産現場において、数多くのロボットが協調して一斉に溶接等の作業を始める光景をご覧になったことのある読者は多いと思うが、安全規格策定の間では、単体のロボットシステムとはどこまでを指すのか、また、一つの指令でこのロボットまでを停止に導く必要があるのか、といった問題が真剣に議論されている。日本が得意とする統合生産システムのような形態に発展してきているロボット分野においては、より高速で、かつ人に対してのみならず、ロボット同士の協調／分散作業を確実に実現することができる安全なネットワーク通信技術が、まさに必要とされているのである。

参 考 文 献

- [1] 特集「ロボットの安全化」, 日本ロボット学会誌, vol.25, no.8, 2007.
- [2] ISO 10218-1: 2006 Safety requirements for robots in industrial environments—Part1: Robots.
- [3] IEC 60204-1: 2005 Safety of Machinery—Electrical equipment of machines—Part1: General requirements.
- [4] IEC 61508-2: 2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.
- [5] BS EN 50159-1, 2: 2001 IEC-62280-1, 2: 2002 Railway applications—Communication, signaling and processing systems—Part 1: Safety-related communication in closed transmission systems, Part 2: Safety-related communication in open transmission systems.
- [6] J. Rushby: A Comparison of Bus Architectures for Safety-Critical Embedded Systems, Technical report, NASA, 2003.
- [7] K. Driscoll and K. Hoyme: "SAFEbus [for avionics]," Aerospace and Electronic Systems Magazine, IEEE, vol.8, no.3, pp.34-39, 1993.
- [8] H. Kopetz: "Fault Management in the Time Triggered Protocol (TTP)," Euromicro 1994, pp.4-11, IEEE Press, 1994.
- [9] C. Scheidler, G. Heiner, R. Sasse, E. Fuchs, H. Kopetz and C. Temple: "Time-Triggered Architecture (TTA)," European Multimedia, Embedded Systems and Electronic Commerce (EMMSEC), 1997.
- [10] G. Bauer and H. Kopetz: "Transparent Redundancy in the Time-Triggered Architecture," Proc. Int. Conf. on Dependable Systems and Networks, 2000.
- [11] H. Kopetz and G. Bauer: "The Time-Triggered Architecture," Proc. IEEE Special Issue on Modeling and Design of Embedded Software, 2003.

山田陽滋 (Yoji Yamada)

1983年3月名古屋大学工学研究科修士課程修了。同年4月豊田工業大学助手勤務。1992年工学博士(東京工業大学)。1993年豊田工業大学助教授。同年Stanford University 客員研究員。2004年4月から現職。知能システム研究部門安全知能研究グループ長。これまで、ロボットのセンサ・通信・知的制御に関する研究、および、人間／ロボット共存系による安全・協調技術の研究に従事。

(日本ロボット学会正会員)

中坊嘉宏 (Yoshihiro Nakabo)

2000年東京大学大学院工学系研究科計数工学専攻博士課程修了。同年、同大学リサーチ・アソシエート。2002年理化学研究所バイオ・メテックコントロール研究センター研究員。2005年より産業技術総合研究所知能システム研究部門安全知能研究グループ研究員。これまで、1ms超高速ビジョン、人工筋肉、人と共存するロボットのための安全知能の研究に従事。(日本ロボット学会正会員)

齋藤 元 (Hajime Saito)

1996年University of Sussex, Cognitive Sciences, Knowledge Based Systems MSc 修了。1998年株式会社童夢入社。レーシングカーの電装、実験装置、ソフト等担当。2002年独立行政法人産業技術総合研究所知能システム部門ヒューマノイド研究グループ特別研究員を経て、2005年ゼネラルロボティクス株式会社開発部専任となる。機械を自由に動かせるようにすることに興味がある。

(日本ロボット学会正会員)