組込みシステムのこれから

名古屋大学 未来社会創造機構 教授
大学院情報科学研究科 附属組込みシステム研究センター長
高田　広章

これからの組込みシステムは，ネットワークを経由してクラウドと接続され，全体としてより高度なサービスを提供するようになるだろう。そのときの課題として，ディペンダビリティの確保と機能配置の最適化を挙げることができる。本稿では，それらの課題について紹介し，取り組む必要のある技術について述べる。

1 はじめに

情報化社会という言葉が表す通り、過去 10 年の間に、我々の社会生活は、情報技術（IT）に依存したものとなってきた。情報化社会は、社会の利便性や効率化に大きく貢献した一方で、サイバーセキュリティの問題など、過去にはなかった課題をもたらしている。

これからの 10 年は、IT に加えて、組込みシステム技術（Embedded Technology;ET）への依存が加速するものと思われる。M2M（Machine to Machine）や IoT（Internet of Things）という用語が注目されている通り、組込みコンピュータに制御された「機械」や「モノ」が、ネットワークを経由してクラウドに接続される。クラウド（情報システム）は、組込みシステムを通じて物理的な世界とつながることで、より高度なサービスを提供するようになるだろう。ここでは、クラウドと組込みシステムがつながったシステムを、統合システムと呼ぶことにする。

統合システムが提供するサービスは、社会の利便性・快適性の向上や効率化に加えて、サステナビリティや安全・安心にも貢献する。例えば、スマートグリッドは、電力供給の安定化により安全・安心に貢献することに加えて、再生エネルギーの活用や省エネルギー化により、サステナビリティにも貢献する。また、ITS は、より安全な道路交通システムの実現に貢献することに加えて、渋滞を減少させることで、道路交通の効率化や省エネルギー化にも貢献する。

ここでは、社会インフラとなる大規模な統合システムが構築されていく流れの中で、組込みシステム技術が果たすべき役割と、取り組むべき技術課題について述べる。

2 高度なサービスの創出

統合システムにより高度なサービスを創出するために重要な 2 つのキーワードが、コネクティビティとビッグデータである。

コネクティビティは、統合システムを成り立たせる大前提である。数多くの小規模な組込みシステムを安価に（また、小さい電力消費で）ネットワーク接続するためには、これまでとは違った種類のネットワーク技術（例えば、Wi-SUN のような）が必要である。また、あらゆる「モノ」を接続してサービスを提供するためには、プロトコルの標準化（例えば、ECHONET Lite のような）も重要な課題である。これらの課題は、徐々に解決されていくと思われる一方で、コネクティビティが確保されることにより、組込みシステムもサイバーセキュリティの問題から無縁ではいられなくなる。

ビッグデータに関しては、組込みシステムは、その入

口と出口の役割を果たす。ビッグデータの生成源の多くは組込みシステムであるし、その処理結果は、組込みシステムを通じて物理的な世界にフィードバックされることもある。ビッグデータの処理自身は、大きいメモリ容量と処理能力が必要であることからクラウド上で行うことになる。

3 クラウドと機能配置の最適化

すべてのコンピュータがネットワークで接続されると、計算処理はどこで行ってもよくなる。つまり、ネットワークによる機能再配置が起こる。例えば、カーナビゲーションシステムを例に取ると、従来はナビゲーションユニット内のハードディスクなどに地図を格納し、そのユニットのプロセッサで経路の探索を行っていたが、こういった処理は、サーバー（クラウド側）で行う方がメリットが大きいため、今後は、サーバーで行うケースが増えていくだろう。

一方で、すべての処理をクラウドで行って、組込みシステムは単なる入出力装置（端末装置）になるかと言うと、幾つかの理由により、そのようにはならないと考えられる。

1つの理由は、ディペンダビリティとリアルタイム性の確保である。ネットワークの信頼性や速度が上がっているとは言え、100% の保証は難しく、高いディペンダビリティが求められるサービスの処理を完全にサーバーに委ねるのは、今後も容易ではないと思われる。これについては、次の節で詳しく議論する。

2つめの理由は、消費エネルギーである。一般に、高性能なコンピュータ（サーバー）は、低性能なコンピュータ（組込みシステムの多く）と比べて、エネルギー効率が悪い。ポラックの法則を準用すると、性能が n 倍のプロセッサのエネルギー効率は、おおよそ n 分の 1 ということになる。実際、クラウドサービスのためのデータセンターは、膨大な電力を消費している。また、情報を運ぶためにもエネルギーは必要である。ある試算によると、このままインターネットの通信量が増え、かつルータのエネルギー効率が変わらないと、2020 年代にはルータの消費電力が全発電電力を超えるという結果が得られている [1]。

以上のような理由により、すべての処理をクラウドで行うようにはならないと考えられる。上記の観点からは、むしろ、組込みシステムで処理した方が利点が大きいわけだが、一方で、ビッグデータを使用する処理の場合、組込みシステムに大規模データを置いておくことは難しい。この問題に対しては、生のビッグデータはクラウドで処理し、ビッグデータに処理を加えた結果（大きくないデータ）のみを組込みシステムに持たせるアプローチが考えられる。いずれにしても、クラウドと組込みシステムの間で、最適な機能配置を行うことが重要である。

この最適機能配置を実現するための技術として、2つのアプローチがある。1つは、統合システム設計の早い段階で、システムをモデル化して評価を行い、最適な機能配置を決定する方法である。もう1つのアプローチは、機能配置を柔軟に変更できるようなプラットフォームを用い、機能配置の決定を、設計のできる限り遅い段階で行う方法である。例えば、車載制御システム向けのソフトウェアプラットフォームの標準である AUTOSAR[2] では、車載コンピュータ（ECU）の間での機能配置を柔軟に行えるような仕組みが導入されている。ただし、クラウドとの間の機能配置最適化までは想定されておらず、今後の課題である。

4 ディペンダビリティの確保

大規模な統合システム全体を、高い信頼性で構築するのは極めて難しい（できたとしても、膨大なコストがかかる）。とくに、複数のベンダによるシステム／サービスが接続された場合、サービス全体で責任を持つ者がいなくなる可能性もあり、高い信頼性を期待することができなくなる。また、前に述べたように、高い信頼性やリアルタイム性を、ネットワークを超えて保証するのは難しい。

そこで、例えば人命がかかっているなど、高い安全性が求められるサービスにおいては、安全性にかかわる部分は組込みシステム単独で担保する（言い換えると、クラウドやネットワークが誤動作／動作停止しても、安全性にかかわる事態にならないようにする）のが、有力なアプローチである。そのため、電子システムの安全性を確保するための機能安全の技術は、今後も、組込みシステムの最重要技術である。

とは言え、このアプローチだけでは、実現可能なサービスが限定される。例えば、車車間通信により車の現在位置を通知することで、車同士の衝突を防止するサービスを考える。この場合、他車からのメッセージにより衝突が予想されると、車にブレーキをかけて停止させたいが、他車からの間違ったメッセージを信じてブレーキをかけると、むしろ危険である（後ろの車に追突される可能性がある）。そのため、上記のアプローチ（ネットワークに依存せずに安全性を確保する）を厳密に守ると、このようなサービスは提供できない。更に、この例にも当てはまるが、他社が開発したシステムからのメッセージを信じてよいかという問題も含んでいる。

そこで、クラウドやネットワークの誤動作によって安全性が脅かされる場合には（あくまで誤動作（integrity を失った状態）であって、クラウドやネットワークが動作しないこと（availability を失った状態）で安全性が脅かされる場合は更に難度が高い）、通信相手の認証により、ディペンダビリティを確保するアプローチがある。具体的には、通信相手が他社が開発したシステムである場合には、まず、通信相手となるシステムが定められたディペンダビリティ基準を満たして開発されているかの認証を受けた上で、通信している相手が確かにその認証を受けたシステムであることを認証するという、２つの認証を行う。後者の認証については、公開鍵基盤（Public Key Infrastructure; PKI）を用いることができる。

前者の認証については、車車間通信を対象に、通信相手となるシステムが満たすべきセキュリティ基準をレベル分けして定めた信用保証レベル（TrustAssurance Level; TAL）という考え方が提案されている [3]。今後、異なる会社が開発したシステムを接続する必要がある他のアプリケーション領域に対しても、同様の考え方が導入されていくものと思われる。

5 今後に向けて ～アーキテクチャ重視の必要性～

以上で述べたように、これからの 10 年、組込みシステムがクラウドにつながっていく過程で、ディペンダビリティの確保や機能配置の最適化といった課題に取り組んでいくことが必要である。

複雑化するシステムを設計する中で、このような課題に取り組む際には、システムのアーキテクチャ（または、設計コンセプト）を整理して取り組むことが不可欠である。我が国のシステム開発は、開発現場からのボトムアップ型の開発で強みを発揮してきたが、複雑化するシステムを効率的に開発するためには、アーキテクチャから考え始めるトップダウン型の考え方を取り入れることが不可欠である。例えば、ディペンダビリティの確保に関しても、システムのどの部分にどの責任を負わせるかを体系的に設計しないと、対策の漏れや、逆に重複対策が避けられない。

そのためには、プロジェクトマネージャとアーキテクトを分離し、アーキテクトに権限を与える（IT の分野では最近増えていると聞くが、組込みシステムの分野では例を聞かない）など、開発体制からの見直しが不可欠であると考えている。

【参考文献】

[1] http://www.aist-victories.org/jp/about/outline.html

[2] http://www.autosar.org/

[3] A. Kiening, D. Angermeier, et. al.: Trust assurance levels of cybercars in v2x communication, Proc. of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles, pp. 49-60, 2013.