ISS-P-103

LL/SC 命令を用いた REMON によるスタックオーバーフロー検出

濱中　貴弘†　　南角　茂樹†
† 大阪電機通信大学大学院　総合情報学研究科コンピュータサイエンス専攻

1. はじめに

近年、産業機器のみならず、家電機器や自動車の各種制御機器、自動販売機などの多くの機器の制御には、組み込みソフトウェアが利用されている。そして、通信技術の発展、通信機器の高速化に伴い、組み込みコントーラやセンサなどの機器同士が通信を行い、最適な動作を行う M2M(Machin to Machine)や IoT(Internet of things)技術が注目されている。組み込みシステムは、現実世界の変化に対応して処理を行うことが重要であり、割り込み処理を用いて変化に対応する。割り込みは CPU ハードウェアから呼び出され、実行される。割り込みには、優先度を設定することができる。さらに、割り込み処理の実行中に高い優先度の割り込みが発生した場合、実行中の割り込み処理を一時停止して、優先度の高い割り込み処理に制御を移す多重割り込みを利用した多重処理が利用されている。そして、多重処理を行うためには、排他制御が必要となってくる。

一方、小規模の組み込み機器ではメモリ制約があり、20.4%の組み込み機器では、Real-Time Operating System(以下 RTOS)を搭載していない[1]。そのため、多重処理の実現にためにタスクではなく割り込み処理を利用している。割り込み処理においては、必要なスタック領域がシステム生成時に割り当てられている。しかしながら、ユーザーの設計不備や使用環境下での想定外の割り込み処理の呼び出しにより、割り当てられたスタック領域以上に使用してしまう場合がある。これがスタックオーバーフローである。スタックオーバーフローが発生した場合、他の領域を破壊してしまい、システム全体に問題を及ぼす結果となる。

2. 現状の問題点

RTOS を使用している場合であればタスクのスタックオーバーフローの検出は可能である。しかし、割り込み処理スタックのオーバーフローの検出はできない。なぜなら、タスクは RTOS の制御下にあるのに対して、割り込み処理は RTOS よりも優先度が高いためである。また、すべての割り込みが一つのスタックを使用しているため、個々のスタック領域が明確ではない。そのため、割り込み処理ソフトウェア自体の不具合やハードウェアの不具合、想定以上の割り込み処理呼び出しによって、割り当てられた領域以上のスタックを使用してしまい、他の領域を破壊してしまう。さらに、スタックオーバーフローがどの割り込みで発生しているかの判定が難しく原因追求に時間を要する。

3. 提案手法

提案方式では、タスク呼び出しを行った際にスタックの終端部に対して、Load-Link 命令を配置してメモリへのアクセスを監視する。そして、タスク終了時にスタックオーバーフローを Store-Conditional 命令を用いて終端部に対してアクセスがあったかを検査する。これにより、スタックオーバーフローの検出を行う。スタックオーバーフローが検出された場合は、発生させた割り込み処理のステータスを変更し、システムの停止を行う。各割り込み処理に対して、スタックオーバーフローを検出することが可能となるため、スタックオーバーフローを発生させた割り込みの特定を迅速に行うことができる。

4. まとめと今後の予定

本研究の提案システムを用いることで従来の REMON[2]のマジックナンバー方式[2]を用いたスタックオーバーフローの検出では、予め設定したマジックナンバーとスタックオーバーフローによって書き込まれた値が同一であった場合のスタックオーバーフローが検知不可能であった問題が解決する。これにより、従来方式では検出できなかったスタックオーバーフローも検出することができ、どの割り込みでスタックオーバーフローが発生したかも知ることができる。

今後の予定としては、提案システムの実装と検証を行う。また、従来のマジックナンバー方式、他の RTOS との実行時間の比較やスタックオーバーフローの検出率も測定し、有用性を示していきたいと考えている。

参考文献

[1] 経済産業省:「2010 年版組み込みソフトウェア産業実態調査報告書」(2011)

[2] 南角茂樹、水篠公範、小泉寿男、福田晃:「組込みシステム用割り込みスケジューラ REMON」、電気学会論文誌 C(電子・情報・システム部門)Vol.133 No.2 pp.316-325(2013-2)

[3] 南角茂樹、川上博行、小泉寿男、福田晃:「割り込みスケジューラ REMON のスタックオーバーフローの制御機能」、電気学会論文誌 C(電子・情報・システム部門誌)、Vol133 N0.8 pp.1509-1520(2013-8)