

2007年4月17日
株式会社ヴィッツ
NPO 法人 TOPPERS プロジェクト
アイシン精機株式会社
株式会社東海理化電機製作所
アイシン・コムクルーズ株式会社

保護機能 OS の実証実験を開始

～保護機能 OS の実用性・安全性を検証し、次世代車載ソフトウェア開発に
必要なプラットフォームを考える～

地域新生コンソーシアム研究事業「自動車統合制御用組込みOS」の中心企業である株式会社ヴィッツは、同コンソーシアムの研究実施者であるアイシン精機株式会社、アイシン・コムクルーズ株式会社¹とアドバイザーである株式会社東海理化電機製作所と協力し、「自動車統合制御用組込みOS」の最も重要な研究開発成果である保護機能OSの実証実験を開始しました。

このコンソーシアム研究事業では、名古屋大学、(株)ヴィッツ、東海ソフト(株)、(株)サニー技研、名古屋市工業研究所、(株)豊通エレクトロニクス、アイシン精機(株)らの研究実施者が、トヨタ自動車(株)、(株)東海理化電機製作所、アイシン・エイ・ダブリュ(株)らのアドバイザー協力を得て、自動車統合制御向けの組込みOSの開発を実施しています。2006年度～2007年度の2年間で、次世代の自動車制御システム向けのプラットフォームの標準化を目指して、保護機能を持った組込みリアルタイムOS、車載通信ミドルウェア、検証スイートの3つのサブテーマを、(株)ルネサステクノロジ製のマイコンを使用して開発してきました。2006年11月末に、前記サブテーマのうち、車載通信ミドルウェアの実証実験を、実車を用いて機能検証を行いました。

保護機能OSは、メモリ保護機能と時間保護機能を有しています。

メモリ保護機能は、汎用OSでは広く利用されている安全性機能ですが、組込み機器においては、組込み機器が求めるリアルタイム特性との関係で、一般的に実用化されていない機能です。本研究事業では、組込みシステムの特徴を利用し、リアルタイム特性を維持したまま実現できるメモリ保護機能の開発²に成功しています。

時間保護機能として、デッドラインモニタリング方式の時間保護と階層型スケジューラ方式と呼ばれる時間保護の2種類の時間保護機能の開発に成功しています。デッドラインモニタリング方式は、単純に時間制限内に特定処理が完了していない場合の動作不良を防ぐタイプの時間保護です。階層型スケジューラ方式は、処理単位に許される実行可能時間を動的に管理する時間保護であり、デッドラインモニタリング方式では検出できない不良原因を特定できる時間保護機能です。

これらの保護機能が有効に機能することにより、自動車制御ソフトウェアが抱える問題点（ECU搭載個数の増加、ワイヤーハーネス重量の増加）を解決/改善するために期待されるECU統合を容易にする基本機能を提供することができます。また、近年、組込みソフトウェアで導入が検討されている機能安全規格が基盤ソフトウェアに求める安全機能の一部を提供することができます（監視、安全処置の機能部位を他の部位から隔離し、安全を担保するための技術として）。

今回開始した実証実験の第2ステップは、保護機能OSの実用性・安全性の確認と保護機能OSに求める要求条件の過不足等を検証するために車を用いた実証実験を行う予定です。

アイシン精機とアイシン・コムクルーズは、保護OS（メモリ保護、時間保護）を用いて、保護機能の有効性や

¹ 2007年2月1日ソフトウェア開発を中心とするアイシングループの会社として設立。本研究参画メンバーの移動もあり、今後はアイシン・コムクルーズとしても協力していただけることとなりました。

² 本メモリ保護機能は、組込みOSのみで実現しているのではなく、プロセッサ内部にリアルタイム特性を維持できる保護機能用部品（MPU; Memory Protection Unit）を新規開発し、ハードウェアとソフトウェアが協力して実現している機能です。MPUの開発はルネサステクノロジ社の協力をえています。

実用性についての検証を行います。

東海理化は、自社類似製品を、時間保護を用いた機能統合を実施し、安全かつ容易に実装可能であるかを検証します。

尚、実証実験の最終確認検証は2007年秋頃を予定しています。

ルネサス テクノロジ 取締役 マイコン統括本部 本部長 武部 秀治 氏のコメント

次世代の自動車技術に必要な保護機能を有する基盤ソフトウェアの実証実験に半導体メーカーの立場から全面的に協力いたします。我々半導体メーカーにとっても、自動車制御技術の動向は注視する必要があり、特に、ECU 統合技術や安全性の担保技術は大変重要であると考えています。今回の保護機能 OS で、特に、メモリ保護機能については、その研究過程で、当社のプロセッサと特注である MPU (Memory Protection Unit) を利用していただいています。今後、自動車制御技術にはメモリ保護や時間保護といった機能が必須となることは明らかであり、当社としても各種保有技術を業界に提案を実施したいと考えています。そのため、当社では今回の研究および今後の実証実験には全面協力をし、プロセッサが担う保護機能の早期実現をめざします。

アイシン精機 電子系技術部 副部長 鈴木 延保 氏のコメント

自動車の電子制御部品においては、高機能化に伴う、開発規模の増大、通信複雑度の増加、統合化や機能安全への対応など、製品のアプリケーションソフトの開発技術と検証への要求は年々高まっています。

そのような状況で基盤ソフトウェアに保護機能を取り入れることは、我々の抱える課題のひとつを解決するための大きな期待があります。今後の実証実験で、今回技術開発が完了した保護機能 OS の改良点などを少しでも洗い出し、実製品に利用できるようにフィードバックをかけ、標準基盤として応用の出来る保護機能 OS となるよう協力して行きます。当社はこの保護 OS を自社製品に適用検討していきたいと考えています。

東海理化 エレクトロニクス技術部 プラットフォーム開発室 室長 伊藤 茂二 氏のコメント

ボディ系電装部品メーカーの立場として、地域新生コンソーシアム研究事業で保護機能 OS が開発され、さらに、保護機能の実証実験を行うことに大きな期待をしています。今回実証実験を検討されている保護機能 OS は、当社が担っている多数のボディ系電装部品を安全にかつ容易に実装するために貢献できる技術と考えております。また保護機能 OS は安全性を必要とする重要なソフトウェア部位を隔離する機能も持ち合わせています。当社はこのような性質を持ち合わせる基盤ソフトウェアを製品に取り入れていくことを視野に入れ、今回の実証実験を含め協力をする予定です。

名古屋大学 大学院情報科学研究科 教授 高田 広章 氏のコメント

「自動車統合制御用組込み OS の開発」プロジェクトリーダーの立場から、実証実験の実施や製品化検討を心から感謝いたします。参加企業のご尽力により、当初予定以上の成果（2006/11 に実施した通信ミドルウェアの実証実験やアイシン精機殿の製品適用予定など）を得られたと考えています。さらに、今回、研究に参加していただいた企業が、公的予算事業期間完了後も継続的な活動をしていただけることにプロジェクトリーダーとして感謝いたします。有志メンバーの努力に報いるためにも、プロジェクトリーダーとしても、この実証実験が成功に終わるよう、可能な限りの技術的な支援を約束するとともに、今回開発した保護機能 OS が日本の自動車産業において、標準ソフトウェアの候補として採用されるための努力をしたいと思っております。

お問い合わせ先

本発表に関するお問い合わせは、以下にお願いします

株式会社 ヴィッツ 開発第3部（担当：服部）

〒460-0008 名古屋市中区栄 2-13-1 第2白川ビル 7F

TEL: 052-223-7570 / 052-218-5855

Email: hat@witz-inc.co.jp