2006 年 11 月 15 日
株式会社ヴィッツ
NPO 法人 TOPPERS プロジェクト

機能安全対応自動車制御用プラットフォームの開発を開始

～中部地区中小企業が機能安全対応プラットフォームの標準化を狙う～

株式会社ヴィッツと名古屋大学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が中心となり、中部地区に拠点を持つ中小企業である 東海ソフト株式会社、株式会社サニー技研 と公設機関である 産業技術総合研究所 システム検証研究センター、名古屋市工業研究所、北海道立工業試験場 らがコンソーシアムを形成し、トヨタ自動車株式会社、アイシン精機株式会社、アイシン・エィ・ダブリュ株式会社、株式会社東海理化電機製作所、株式会社ルネサステクノロジ、株式会社豊通エレクトロニクスらのアドバイザ協力を得て、機能安全 (IEC61508 SIL-3 を想定) 対応自動車制御向けのソフトウェアプラットフォームの開発プロジェクトを開始します。この開発プロジェクトは、経済産業省の平成 18 年度 戦略的基盤技術高度化支援事業 (中小企業基盤整備機構) に採択されており、総括研究代表者は名古屋大学 大学院情報科学研究科 教授 高田広章が努め、副総括研究代表者および事業管理者を株式会社ヴィッツが務めます。

このプロジェクトは、次期自動車制御システム開発で必要になると考えられている、機能安全に対応した自動車制御システム向けのプラットフォームを開発し、プラットフォームの標準化を目指します。この開発では、機能安全に対応した安全機能 OS (単に、既存の基本ソフトウェアを機能安全規格に対応するばかりでなく、現在の産業界で実現されている安全対策を基本ソフトウェアに取り入れる動作安全にも対応する) 、機能安全に対応した現世代および次世代の通信ミドルウェア (CAN/ LIN/ FlexRay) 、機能安全に対応した次世代例示アプリケーションおよび対象サンプル車両、機能安全対応ドキュメントの４つのサブテーマで開発を行います。
なお、本事業で開発したソフトウェアおよびドキュメントは NPO 法人 TOPPERS プロジェクト (以下、TOPPERS プロジェクト) からオープンソースとして公開を予定しています。

ここで述べる機能安全とは、欧州が中心となり策定した機能安全規格 (IEC61508) を指します。これは、1970 年代の一連の大事故が引き金となり、原因発生責任者 (Liability) 、保証原則 (原状回復主義) 、リスク受容による公平性を確立するために規格化されました。
自動車産業および他の機械産業において、今後これらの安全規格は製品制作上必須になる可能性が高いとの判断がされています。

安全機能 OS とは、基本ソフトウェアである OS に安全機能を取り入れることにより、OS 上で動作するアプリケーション状況の管理・確認の実施や、OS 自身が正しく動作しているなどの確認を動的に管理する機能です。これらの機能は、現在の自動車や他の産業機械にも含まれている機能ですが、通常、これら機能はアプリケーションで実施し、その製品毎に管理方法や期待できる安全性が異なります。その結果、システム全体での安全性を保障するために多くの労力を必要とします。安全機能 OS を利用することで、従来のアプリケーションでは管理しきれない、アプリケーション相互間や OS の動作状況まで安全に管理することが可能となり、システム全体で安全に動作することが可能となります。安全機能 OS の開発にあたっては、TOPPERS プロジェクトの次期標準 OS である TOPPERS/ASP カーネルをベースとします。

通信ミドルウェアのサブテーマでは、現在の車載ネットワークとして最も広く利用されている CAN および LIN 通信のミドルウェアの開発と次世代の車載ネットワークで業界標準となる FlexRay 通信ミドルウェアを対象とます。いずれのミドルウェアも TOPPERS プロジェクトから公開もしくは公開を予定しているミドルウェアをベースとし機能安全に対応します。例示アプリケーションおよび対象サンプル車両は、機能安全対応を検討するための対象製品として開発し、オープンソース公開後に必要とする企業が自由に利用できる対象装置として開発します。

機能安全対応ドキュメントとは、本研究で取り組む機能安全対応過程を記したドキュメントを示します。こ

れは、国内企業が機能安全対応を容易に実現するための資料として提供する予定です。

この開発プロジェクトにより、次期自動車開発および次期産業機器開発が抱える次のような問題を軽減／解決することができます。

(1) ソフトウェアの安全性
現在の自動車制御システムでは、アプリケーション毎のポリシーにより、アプリケーション部位でソフトウェアの安全性を確保しています。この方法では、システム全体で統一されたポリシーでなく、またアプリケーションにより安全性は異なります。安全機能 OS を導入することにより、システムの安全性に対する考え方が統一され、ソフトウェアの安全性に関する問題が軽減／解決できます。
また、本効果は自動車開発ばかりでなく、他の産業機器にも利用できます。

(2) 機能安全対策および対策コスト
国内での機能安全対策ソフトウェアの開発事例はありません。そのため機能安全対策に必要な作業やコストなどが明確になっておらず、大きな不安と困惑が国内産業に広がっています。本開発において、基本 OS、通信ミドルウェア、例示アプリケーションを機能安全対策することにより、機能安全対策方法を明確にします。また、対策方法や各種ドキュメントを開発し公開することにより、機能安全対策および対策コストに関する問題を大幅に軽減／解決できます。
また、機能安全対策済みのソフトウェアプラットフォームをオープンソースとして公開することにより、多くの産業界において無償で機能安全対策ソフトウェアの入手が可能となり、導入コストの大幅な削減が実現できます。

この開発プロジェクトで開発したソフトウェアおよび各種ドキュメントは、自動車制御システムの分野でデファクト標準とすることを狙って、オープンソースソフトウェアおよびドキュメントとして、TOPPERS プロジェクト(http://www.toppers.jp/)から公開します。また、自動車制御システム向けのプラットフォーム技術の標準化を行うために、国内の自動車メーカを中心に設立された JasPar (http://www.jaspar.jp/) へ、標準的なソフトウェアおよびドキュメントとして提案することも視野に入れています。

トヨタ自動車 統合システム開発部 城戸正利氏のコメント

大学とソフトウェア企業が中心となり、経済産業省のご支援を得て、自動車制御システム開発が抱える機能安全に対応されることを、自動車メーカの立場から歓迎したいと思います。我々は、ここで開発および検討される機能安全対応手法と機能安全に対応した安全機能 OS 技術は、自動車メーカが競って開発するよりも、共通で利用するのが望ましいと考えています。開発および検討されたソフトウェアやドキュメントがオープンソースとして公開されることで、自動車メーカや各種産業機械分野で共通に利用できる基盤ソフトウェアに成長することが期待できると思います。自動車向け機能安全規格には、IEC61508 の他に ISO26262 が国際的に検討されています。この開発プロジェクトでは自動車メーカの立場で、自動車メーカが求める機能安全要求などを伝えることで、ご協力したいと考えています。

アイシン精機 電子系技術部 鈴村延保氏のコメント

自動車電装部品に用いられる、基盤ソフトウェアの機能安全対応技術の開発と普及が、今回の支援事業で発展すると期待しています。
市場のグローバル化に伴い、機能安全を代表とした、国際標準規格に準じた取り組みがより求められています。それらに対応でき、また高度な制御ソフトウェアを効率的に開発出来るプラットフォーム標準化を希望していますが、現状では、自動車メーカ毎に利用する基盤ソフトウェアが異なります。
当社はこの研究開発が、国際標準のプラットフォーム技術と、機能安全設計指針となることを期待し、製品適用に向けたアドバイスや検証に参加します。

株式会社ヴィッツ 代表取締役 安場尚一のコメント

今回採択された研究事業は、自動車産業にとっても弊社の今後にとっても重要なテーマであり、全社一丸でこの研究事業を成功させたいと考えております。この研究事業において、弊社は副総括研究代表者と事業管理者であります。これは研究ばかりでなく研究運営を円滑に進める母体でもあります。日本政府が中小企業のものづくり産業を支援する法案の施行を行い、国を挙げて中小企業の技術力の底上げを支援されております。本年度から開始された戦略的基盤技術高度化支援事業を実施するにあたり、来年度以降に研究を行う企業の見本となるような成功を収める努力を尽くすことを約束させていただきたいと思います。

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
総務部：安場、佐藤　　（技術的内容；開発第 3 部：服部 ）
TEL: (052) 220-1218　(開発第 3 部: (052) 223-7570)