2013 年 11 月 20 日
株式会社ヴィッツ
NPO 法人 TOPPERS プロジェクト

機能安全開発の大幅コストダウンが可能！

パーティション OS 一般公開開始

～ 異なる安全度水準(SIL/ASIL)の混在が可能に ～

株式会社ヴィッツは、パーティショニング機能を取り入れた高信頼システム対応リアルタイムオペレーティングシステム（RTOS）の開発に成功しました。また、その RTOS を NPO 法人 TOPPERS プロジェクトから「TOPPERS/PARK ～BCC Light～」の名称で、2013 年 11 月 20 日より一般無償公開致します。

無償公開物は、TOPPERS/PARK ～BCC Light～のソースコード、Safety Concept ドキュメント、Safety Requirements Specification ドキュメント、TUV レポート（IEC 61508 SIL3 Capable）など、機能安全の製品認証に必要なドキュメントを含んでいます。

なお、この RTOS 開発は、経済産業省の研究事業である平成 22 年度 戦略的基盤技術高度化支援事業の採択を受け、研究した成果を活用しています。

本 RTOS には、株式会社ヴィッツ、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（NCES)、株式会社 OTSL、NPO 法人 TOPPERS プロジェクトの連名で提案中の「パーティショニング機能に関する標準規格の提案」に準じた「パーティション間の時間保護機能」を搭載しております。本 RTOS を TOPPERS プロジェクトより一般公開することで、提案中の「パーティション間の時間保護機能」を多くの方に実際に使用して頂き、パーティショニング機能の機能性や有用性を検証して頂くことを目的としております。

また、株式会社ヴィッツでは、無償公開物にメモリ保護機能を追加したフルセット版 RTOS の商用販売を計画しています。

本 RTOS の利用を想定している対象システムは、移動支援ロボット、介護ロボット、航空宇宙（飛行機、ロケット）等の安全性（フェールセーフ）や信頼性（フォルトアボイダンス）が求められ、機能停止が許されない高信頼システムです。

一方、安全性の高いシステムにおいてフェールセーフによる安全確保を行う場合、機能安全規格 IEC 61508 では最も安全性の高い SIL 4 適応で二重化などの冗長化技術が必須です。これは単純にシステム構造が複雑化し、開発コストや部品コストが増加する要因となります。更に、自動車では ECU 統合が注目されており、異なる安全性のコンポーネントを同じ ECU に搭載する際には最も安全性の高いレベルに合わせる必要があり、同様に開発コストが増加する要因となります。

本 RTOS では、パーティショニング機能を用いて、対象システムの機能を複数の集合（パーティション）に分けて、空間的・時間的に分離しています。具体的には、安全関連系のパーティションを他の機能のパーティションから保護することで、異なる SIL のパーティションを混在可能に、また変更が発生したパーティションのみの再検証が可能にしています。また、パーティションレベルでの冗長設計が可能となっています。

この度公開する RTOS および関連ドキュメントを用いて当該製品への適用をすることにより、機能安全規格への適応及び、高信頼システム構築の課題であるコスト増加を効果的に抑えることが可能です。

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

近年、機能安全規格への対応が求められる中で、ソフトウェアの開発／検証コストを最適化するために、パーティショニング機能は必要不可欠であると考え、産学連携でパーティショニング機能に関する標準規格の検討を進めてきました。

その成果を実装したリアルタイムカーネルがNPO 法人TOPPERS プロジェクトから無償公開されることを、TOPPERS プロジェクト会長の立場として歓迎します。これをきっかけに、我々の提案した技術が広く活用され、組込ソフトウェア業界の発展につながることを期待します。株式会社ヴィッツが、機能安全対応ソフトウェアに関する技術を蓄積され、今後も引き続き発展されることをお祈りいたします。

株式会社ヴィッツ 代表取締役 脇田 周爾のコメント

この度、弊社はパーティショニング機能を取り入れた高信頼システム対応リアルタイムオペレーティングシステム（RTOS）の開発に成功しました。本 RTOS は機能安全規格への対応によって膨らんでしまう開発コストを抑えるためのカギとなるものであり、その成果を一般公開することで、国内の安全関連ソフトウェアの開発に活用されることを期待しています。

また、弊社では現在、戦略的基盤技術高度化支援事業として「ネットワーク連携が進む次世代自動車・サービスロボット等の利用者安全を保証するセキュリティ基盤ソフトウェアの研究開発」を実施しており、組込みシステムへのセキュリティ対応を進めて行く上で、本 RTOS の活用が必須であると考えています。こちらの事業でも、同様に良き成果報告ができるように最善の努力をしておりますので、今後ともご指導いただけますようお願いします。

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；組込制御開発部：片岡、杉山 ）

TEL: (052) 220-1218