

## 故障未然防衛機能を有した高信頼ソフトウェア プラットフォームの開発を開始

～ 故障未然防衛による安全なソフトウェア開発の新たな試み ～

株式会社ヴィッツは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、産業技術総合研究所らと協力し、故障を未然に防衛する新たな安全機構を取り入れた高信頼ソフトウェアプラットフォームの開発を開始します。このプロジェクトは、経済産業省の平成22年度 戦略的基盤技術高度化支援事業に採択されており、総括研究代表者と事業管理者を株式会社ヴィッツが務め、副総括研究代表を名古屋大学 大学院情報科学研究科准教授 本田晋也が務めます。また、本研究へのアドバイザーとして、名古屋大学、トヨタ自動車株式会社、アイシン精機株式会社、株式会社東海理化電機製作所、オークマ株式会社、株式会社デジタルを迎え、産業界が必要とする故障未然防衛を実現します。

このプロジェクトは、次世代自動車制御システム、サービスロボット制御、次期産業機械・産業ロボット等に求められる安全に関する課題を改善し、当該分野での標準的なプラットフォームにすることを目指します。これらの分野では2005年頃より機能安全規格（IEC 61508 など）の導入が検討されています。

本研究を実施する株式会社ヴィッツと名古屋大学は、平成18年度 戦略的基盤技術高度化支援事業において「機能安全対応自動車制御用プラットフォームの開発」を実施し、自動車向けの機能安全対応プラットフォームの開発に成功しています。機能安全対応自動車制御用プラットフォームは、自動車など復帰が許されるシステムには対応できますが、復帰が許されない航空宇宙などへの適応は更なる対策が必要なが研究を通じて明確となりました。さらに、当該研究から、機能安全には必要と言われている「保護機能」は機能安全対応には必ずしも必要でなく、むしろ、故障検出機能が重要であることが明確となりました。

一方、復帰を許さない高信頼システムにおいて、故障検出機能により故障が検出されても復帰が許されないため、高信頼システムの多くは、故障検出機能だけでは高信頼性を確保できません。このようなシステムには、外乱からの故障を未然に防ぐ防衛機能が有効と考えられ、その機能として「保護機能」が有用であると考えられます。すなわち、高信頼ソフトウェアプラットフォームには、故障検出によるフェイルセーフ<sup>1</sup>だけではなく、フォルトトレランス<sup>2</sup>とフォルトアボイダンス<sup>3</sup>の対策が必要と言えます。

また、株式会社ヴィッツと名古屋大学は、平成17年度 地域新生コンソーシアム研究開発事業において「自動車統合制御用組込みOS」の開発にも成功しています。これは、ECU統合を安全かつ容易に実施できるメモリ保護および時間保護技術の基礎的な研究を実施したものです。この目的は、増加するECU個数を安全かつ容易に削減することを目的とした研究です。そのため、高信頼を目的としているものではありませんが、保護技術の一部の研究成果は、故障防衛機能として活用できると考えます。このECU統合を目的とした保護機能研究は、プロセッサ上で稼動するソフトウェアからの不正メモリアクセスや不正時間消費をソフトウェアプラットフォームで監視および保護した技術です。この研究成果に機能安全規格を導入し、さらに、ダイレクトメモリアクセスなどバス経由の不正アクセスなどプロセッサ周辺装置を含めた保護を実現することにより、高度なソフトウェア・パーティショニング機構を導入し、高信頼システムに利用可能な防衛機能を実現することができます。

すなわち、「機能安全対応自動車制御用プラットフォームの開発」の開発成果である機能安全対応OSに、「自動車統合制御用組込みOS」の開発成果である保護機能を機能安全対応して導入し、さらに、復帰不可時の安全確保手法を取り入れることにより、高信頼システムで利用可能な安全ソフトウェアプラットフォームの開発を実現できます。

<sup>1</sup> なんらかの装置、システムにおいて、誤操作、誤動作による障害が発生した場合、常に安全側に制御すること。

<sup>2</sup> システムの一部に問題が生じても全体が機能停止することなく（たとえ機能を縮小しても）動作し続けること

<sup>3</sup> 故障の生じにくい設計や構造を採用したりすることで、システム全体での障害を回避しようとする考え方のこと。そのための設計技法や管理手法、技術をいう場合もある。

## ループ長 山田 耕嗣氏のコメント

大学とソフトウェア企業が協力し、経済産業省のご支援を得て、サービスロボット実用化の課題の一つである安全関連ソフトウェア技術の開発に取り組まれることを歓迎したいと思います。我々は、ここで新たに開発および検討される復帰が許されない高信頼システムに利用できる故障を未然に防ぐ防衛機能に期待し、さらに、開発成果が安全を必要とする分野で標準的なソフトウェアに育つことに大きな期待を寄せています。このプロジェクトには、サービスロボットメーカーの立場として次世代ロボットが求める安全要求などを伝え、ご協力したいと考えています。

## アイシン精機第1電子系技術部 主査 鈴木 延保氏のコメント

今後、自動車電装部品はますます高度な制御が必要となり、より高い安全性が要求されてきます。よって、次世代の自動車制御に関わる基盤ソフトウェアにおいては、故障未然防衛機能に関する新技術の登場に期待が集まっています。今回の故障未然防衛機能は、既存の車載プラットフォームと国際標準化が進む機能安全技術をベースにし、日本らしいきめ細やかな安全対策による実現を目指して計画されています。日本発の安全技術発信の実現や、国際標準提案に繋がる技術という側面からも期待しておりますので、製品適用に向けたアドバイスや検証にご協力させていただきたいと思っております。

## 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

組込システムが直面している安全課題をソフトウェア技術と機能安全技術を応用し、故障を未然に防衛する研究を開始することをアドバイザーの立場で歓迎します。私自身、基盤ソフトウェア技術を長年に渡り研究開発し、自動車をはじめとした安全ソフトウェア開発の研究も実施してまいりました。このプロジェクトでは研究者としてではなくアドバイザーとしての参加ですが、これまでの研究成果を活用したアドバイスをし、基盤ソフトウェアや組込システムにおける安全技術の確立と活用を本研究から進められるよう協力したいと考えています。

## 株式会社ヴィッツ 代表取締役 脇田 周爾のコメント

今回の研究事業は、日本政府が中小企業の技術力の底上げによる産業活性化を目指す戦略的基盤技術高度化支援事業の一環として採択されました。

本テーマは当社が注力しております自動車産業、次世代ロボット産業、産業機械産業や機能安全事業にとって大変重要であり、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。

当社は、H18年度の戦略的基盤技術支援事業で機能安全に関わるテーマが採択され、その研究途中から、関連事業の事業化を実現しております。また、研究終了後に国際認証機関（ドイツ TÜV-SÜD）から開発成果を利用した「機能安全プロセス認証」を取得しています。

今回の研究採択に於いても前回に負けない成功を収めるべく、この成果を踏まえ努力を尽くすことをお約束致します。

## 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：服部）

TEL: (052) 220-1218