平成 24 年度　戦略的基盤技術高度化支援事業
「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」

研究開発成果等報告書概要版

平成 25 年 3 月

委託者　中部経済産業局

委託先　株式会社ヴィッツ

目次

第1章 研究開発の概要

１－１ 研究開発の背景・研究目的及び目標

【背景】

世界的に高品質を誇る我が国のものづくり産業においても、近年、電子システムが起因する問題が増加傾向にあり（Fig.1）、安全・安心な電子システムの開発が今まで以上に重要になってきている。安全システム開発に関する対策として、欧州では 1990 年代末から**機能安全（ Functional Safety ）**と呼ばれる、電子システムの安全開発に関する規格（IEC 61508 ）が策定され、我が国においても、2006 年頃より注目され始めている。（国家の対応としては、2006 年 4 月 26 日に制定された新法である『中小企業のものづくり基盤技術の高度化に関する法律』の指針に、機能安全が記載されるようになった。また、2006 年 9 月には、IPA/SEC に機能安全部会が設立された。） そのため、本研究提案者らは、2006 年より「機能安全対応自動車制御用プラットフォームの開発」の開発を行ない、**システムの復帰が許される環境下で利用可能な安全性の高いソフトウェアプラットフォームの開発に成功**している。しかし、この研究による成果は、電子システムの復帰を許す条件下での利用を想定し、フェイルセーフによる安全技術によって対応している。すなわち、IEC61508 では、SIL レベルの評価基準に SFF (Safe Failure Fraction) が用いられ、SIL 3 準拠製品であれば、SFF は 99%以上を必要とする。この SFF はハードウェアの故障率を改善することと、故障を検知することにより、SFF 値を上げることとなる（すなわちハードウェアに主眼を置いた考え方である）。しかし、SFF 99% 以上を実現するには、一重系システムでは実質的に実現できず、二重系以上の構成を必要とする。そのため、**復帰が許されない高信頼システム**（航空宇宙、サービスロボットなど）では、システムの二重化など冗長化技術を用いないと利用できない。**冗長化技術を用いると、システム構造の複雑化による開発コストや部品コストが大幅に増大する。**そのため、高信頼システムを安価に開発することができない、という課題が存在する。【課題１】

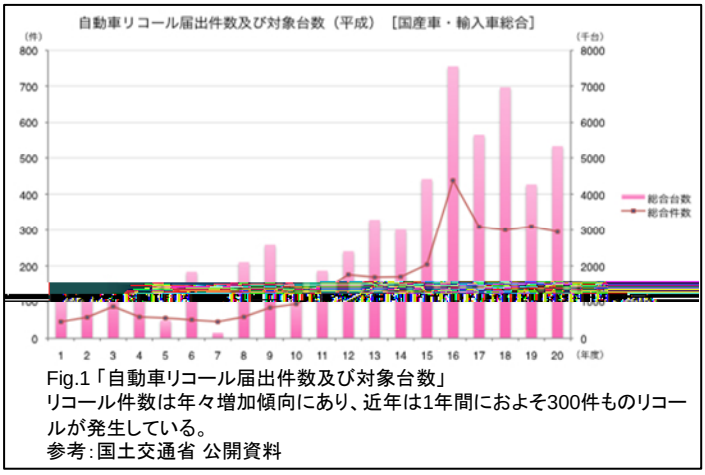


Fig.1「自動車リコール届出件数及び対象台数」
リコール件数は年々増加傾向にあり、近年は1年間におよそ300件ものリコールが発生している。
参考：国土交通省 公開資料

一方、自動車システムを例に挙げると、電子制御装置（ECU）と呼ばれるコンピュータが 1 台につき多いものでは 100 個以上搭載されているが（2006 年 9 月に発表した「レクサス LS460」では約 100 個もの ECU が搭載されたと言われている）、コスト削減のために **ECU 統合**され始めている（Fig.2）。しかし、異なる安全度水準（SIL）のコンポーネントを１つのプロセッサ上に共存させるには**最も安全性の高い SIL に対応した開発を行う必要がある**。すなわち、高安全 ECU と低安全 ECU を統合した場合、低安全 ECU アプリケーションについては**過剰な安全性**を達成する必要があり、**無駄なコストが発生**するという課題が存在する。【課題２】

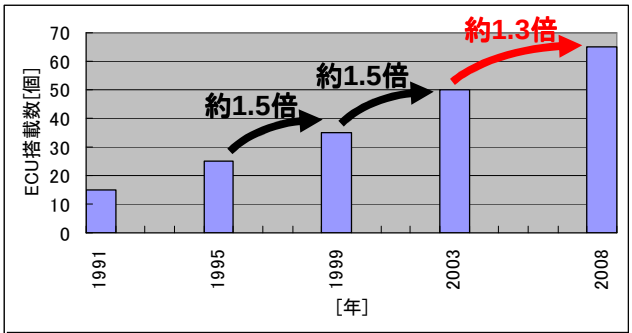


Fig.2「国内高級乗用車のECU搭載数の遷移」
ECUの統合化を進めた結果、増加傾向が緩和されつつある。
参考：Tech-On! トヨタ「クラウン」，ECUの数は減ったのか，増えたのか？

各産業分野において、機能安全対応が急務となっているが、これらの課題を抱えるため、我が国の機能安全対応は国際的にも遅れをとっている。これらの課題を解決するには、**防衛機能とパーティショニング機能を合わせもつ、高信頼プラットフォームが必要**であるが、**国産の高信頼プラットフォームの開発は成功していない。**一方、**海外製の同種プラットフォームはいくつか存在**し、代表的な製品のコストは、導入に１社あたり数千万円以上、

さらに別途ロイヤリティの費用が必要であり、**高価**である。

そこで、本研究では、電子システムのハードウェア障害はソフトウェアでは故障を回避することはできないため、ハードウェア故障検出によるフェイルセーフ技術を用いて対策する。ソフトウェアの不具合やメモリ・CPU 故障によるソフトウェアの誤動作など、ソフトウェアに起因する障害についてはフォルトトレラントとフォルトアボイダンスを取り入れた**防衛機能により障害の伝播・拡大を防ぎ**、さらに**パーティショニング機能によって故障の影響を最小限に留める**ことを可能とした、高信頼ソフトウェアプラットフォームを実現する。

また、この研究の付加的な目的として、**日本発の安全技術基準を考案し、国際認証機関に認可してもらう**ことである。この安全技術基準とは、機能安全規格 IEC61508 の判断基準である SFF 値を、ハードウェア対策を主眼とした方法ではなく、ソフトウェア対策により SFF 値の一部をまかなう方法を模索し、その考え方を日本発の安全技術基準とすることである。

本研究開発には、**高度な機能安全の知識と開発技術が必須**である。研究提案者であるヴィッツは、機能安全国際認証機関である TUV SUD (Germany) から“日本初の機能安全プロセス認証”の監査をパスしており、TUV SUD との関係も良好である。本研究では、国際認証機関の知識を得ながら、防衛機能の機能安全開発を行い、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実現し、日本発の安全技術基準を世界的に普及させる。

【目標】

次世代自動車、サービスロボット、産業機械および産業ロボットなど高信頼を必要とする電子システムへの利用可能な性能を有し、かつ、外乱からの故障を未然に防ぐ「防衛機能」と、万が一故障が発生しても故障の影響の伝播を防ぐ「パーティショニング機能」を付加した高信頼ソフトウェアプラットフォームを実現する。

【技術的目標値】

機能安全規格上、安全度の達成度として故障検出率が重要な指標となる。故障検出は潜在的な故障中であるにもかかわらず、動作継続する危険を防止するために有効である。しかし、故障検出はあくまで故障が発生した後に検出する機能であり、ハードウェア等のランダム故障など防ぎようがない故障については有効な手段である。しかし、ソフトウェアの誤動作に起因する故障の場合も同様に故障後にしか検出できず、例えばソフトウェア故障によるメモリ等の破壊について破壊前に防御することができず、その結果故障の影響範囲を限定できず、安全なシステムを開発することが困難である。

そこで、本研究では、故障検出機能はもちろん、ソフトウェア故障に関する防衛機能を充実させる。具体的には、以下の故障検出率と防衛率を実現する。

故障検出率

対象	現状の検出故障率	目標検出故障率
ランダムアクセスメモリ	80% 程度	90%
リードオンリーメモリ	90% 程度	99%
レジスタ	80% 程度	90%
割込みコントローラ	80% 程度	90%
実行シーケンス	80% 程度	90%
W/D タイマ	80% 程度	90%

防衛率

対象	現状の防衛率	目標防衛率
メモリアクセス	99%	99%
DMA コントローラアクセス	0%	99%
I/O アクセス	0%	99%
処理時間防衛	60%程度	99%
その他分析結果から抽出防衛機能	－	90%以上

上記故障検出率は機能安全規格 IEC61508 等に対策と検出率についての規定が存在し、目標検出率への到達が明確に確認可能である。しかし、防衛率に関する規定は、機能安全規格等には規定されていない。そのため、防衛率への達成率は、安全認証機関等と細密な協議を行い、防衛率到達を検証する予定である。

上記目標を実現するために、以下のサブテーマを実施する。

＜開発サブテーマ内容＞

1. 高信頼ソフトウェアプラットフォームの安全コンセプト開発

復帰が許されない高信頼システムで利用可能な高信頼ソフトウェアプラットフォームに求められる安全コンセプトを策定する。高信頼ソフトウェアプラットフォームに要求される安全をプラットフォームの機能として実現するために、安全アセスメントや安全分析などから障害、防衛対策を抽出し、要求を満たす機能を規定する。策定した安全コンセプトは国際認証機関と協議を行い、目標とする安全性を満たしているかを判断する。

1.1 高信頼ソフトウェアプラットフォームの安全分析

自動車、航空宇宙、サービスロボット、産業機械および産業ロボットなどの復帰が許されないシステムを対象にした安全分析を行う。具体的には、前述システムへの当該ソフトウェアプラットフォームを利用した条件で、ソフトウェアコンポーネントの安全分析を FTA, FMEA, HAZOP 等の手法を用いて安全分析を行う。安全分析の結果から、高信頼ソフトウェアプラットフォームが求める防衛機能や故障検出機能を抽出し、再度分析結果を確認し、故障時の安全対応が十分実施できることを証明する。

1.2 防衛機能検討

高信頼システムに必要な防衛機能の具体的な対応方法を検討する。提案書策定時点で必要と考えている防衛は、メモリ、時間、周辺デバイス等への誤作動の防衛である。これ以外に、前述した安全分析や対象とするシステムで一般化されている防衛などを調査し、防衛機能を決定する。機能安全規格には、分野毎に適した故障への対策が載っている。そのため、各分野の機能安全規格も参考に防衛機能を決定する。（参照規格 : IEC61508 Edition2、ISO26262、ISO13849、IEC62061、ISO10218、JAR/FAR 25 1309、DO-178B など）

本研究を実施する名古屋大学と株式会社ヴィッツは、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」の開発に成功し、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研究を実施している。この研究の目的は、増加する ECU 個数を削減することを目的としており、高信頼を目的としているものではないが、保護技術の一部は「防衛機能」として活用できる。この研究は、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ある。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、外乱からの故障を未然に防ぐ防衛機能を実現できる。

また、故障検出機能により検出した故障を部分的に復帰させるパーティションリブート機能を検討する。「自動車統合制御用組込み OS」の研究で検討したソフトウェア分離機能をベースに欧州で検討が進んでいる AUTOSAR パーティショニング機能との比較調査を行い、各産業で広く使用可能なパーティションリブート機能を検討し、方針を決定する。

1.3 安全コンセプト開発

安全分析結果および防衛機能検討結果をもとに、高信頼ソフトウェアプラットフォームの安全コンセプトを策定する。策定した安全コンセプトは国際認証機関によるレビュー、コンセプトの打ち合わせを実施し、国際認証機関と合意可能な安全コンセプトを開発する。

本研究の最大の課題は、防御機能とその確実性が定量的に判断できないことである。すなわち、従来と同程度のアプリケーション開発コストで、かつ、安全度が異なる複数アプリケーション（タスク）が容易に搭載できる信頼性プラットフォームの安全コンセプトを策定し、その有効性を自己判断しても、国際的な安全対策として基準を満たしているかが判断できない。

本提案代表である株式会社ヴィッツは、「機能安全対応自動車制御用プラットフォームの開発」終了後に自社の活動を実施している。2010 年 3 月時点で、機能安全国際認証機関である TUV SUD (Germany) から“日本初の機能安全プロセス認証”の監査をパスしており、2010 年 5 月の正式認証取得を目指し活動を継続している。この活動において、SafeOS の安全コンセプトも策定しているため、安全コンセプト策定能力は高い。また、TUV SUD との関係も良好であり、本研究における安全コンセプトの策定でも TUV SUD からの支援を得ることができる。

2. 防衛機能の機能安全開発

高信頼ソフトウェアプラットフォームに必要な防衛機能仕様の策定とそのソフトウェア開発を行う。本研究では、具体的なプロセッサとして ARM マイコン（東芝製）を用いる予定である。また、故障挿入試験や周辺機器の評価など特殊な検証を行うために、NIOS II（アルテラ製）を使用する予定である。

尚、ソフトウェア開発は機能安全 IEC61508 SIL3 相当のソフトウェア開発プロセスにて実施する必要がある。株式会社ヴィッツは現在機能安全に遵守した開発プロセスの認証取得の活動をしており、2010 年 3 月時点で既に機能安全国際認証機関である TUV SUD (Germany) から“日本初の機能安全プロセス認証”の監査をパスしている。

2.1 メモリ防衛機能開発

プロセッサに搭載された MPU (Memory Protection Unit) を用い、リアルタイム特性を維持したままのメモリ防衛機能を実現する。MPU を用いたメモリ防衛の基本機能は、H17「自動車統合制御用組込み OS の開発」において、提案者らにより実現している。この研究成果をベースとして、機能安全対応に必要な機能を追加し、さらに機能安全開発プロセスを適用したメモリ防衛機能を実現する。

2.2 時間防衛機能開発

階層型スケジューラ方式を利用した時間防衛機能を開発する。階層型スケジューラによる時間防衛機能も提案者らにより既に基本機能は実現している。本研究では、先の研究成果を基本仕様とし、航空宇宙で利用されているスケジューラ（PikeOS など）との比較調査を行い、最下層スケジューラを改良することも検討する。すなわち、先の研究では、ECU 統合を容易にすることを目的として研究したが、本研究では機能安全側面に立ち、処理間の独立性を高め、時間的干渉や時間的障害防衛を強化した階層型スケジューラを開発する。

2.3 周辺デバイス防衛機能開発

高信頼ソフトウェアプラットフォームを実現するには、周辺デバイスの監視と保護も必要になる。提案者らが ECU 統合を目的に開発した防衛機能では､プロセッサのレジスタ監視とその動作による防衛は実現できているが、レジスタ等を利用せずにメモリにアクセスできるデバイスなどは防衛対象にはなっていない。すなわち、DMA コントローラなどバスに直接つながり動作するデバイスの防衛は実現できていない。しかし、高信頼ソフトウェアプラットフォームにはメモリにダイレクトにアクセスしている周辺デバイスからのメモリ防衛は必須と考えられ、これらの周辺デバイスからの不正処理を防衛する機能を実現する。

尚、本機能実現にあたり、検討したデバイスの他に干渉する恐れが無いことを証明するのは困難な問題となることが予想される。これらの課題対策はハードウェアメーカおよび認証機関等の知識を取り入れて対処することで実現可能と考えている。

2.4 パーティションリブート機能開発

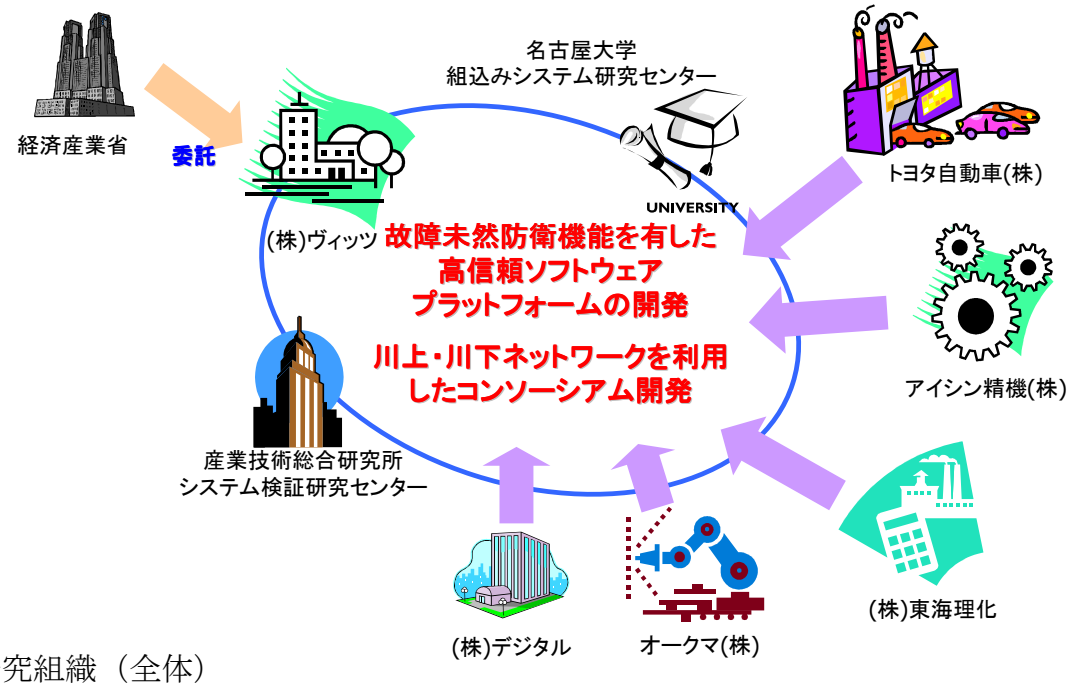
前述までの防衛機能は多種多様な障害を事前に防衛し、障害を発生しない、もしくは拡大しないための機能である。パーティショニングは前述機能と連携して、個別の機能単位を分離し、他への波及を防ぐものであるが、万が一障害を発生した場合には、機能単位で障害を検出し復帰させる機能が必要である。これをパーティションリブート機能として開発する。

この機能は、欧州発標準仕様である AUTOSAR でも仕様化されているが、AUTOSAR 仕様は複雑すぎて、安全機能として利用するには難しいと考える。本研究では、AUTOSAR が提案する仕様を実現することはもとより、さらにシンプルで同程度の機能を実現することを検討し開発する。

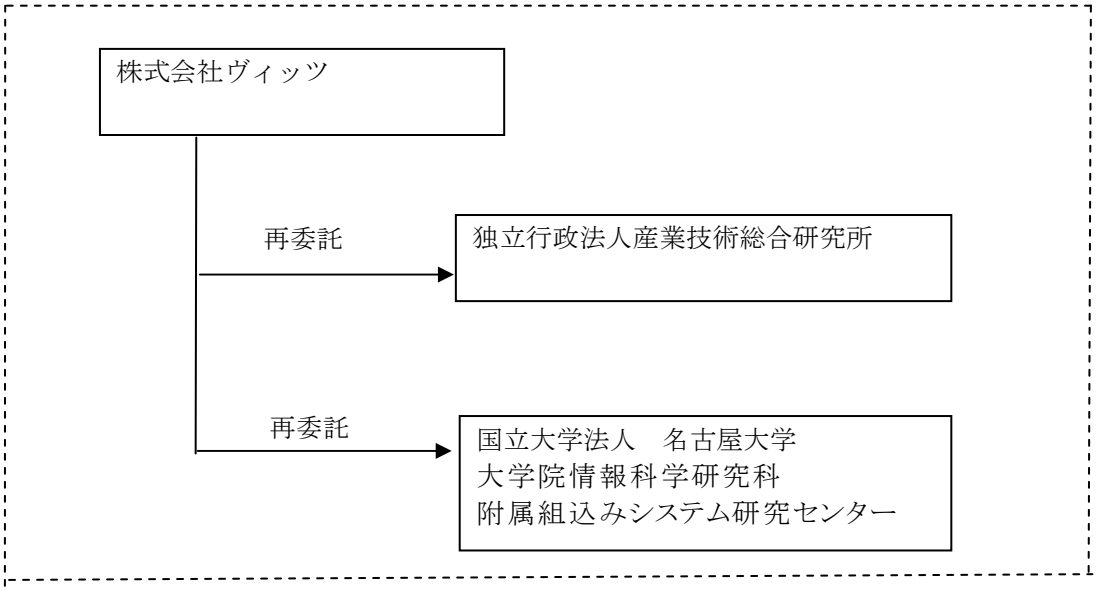
3. プラットフォーム開発

提案者らが既に研究開発した機能安全対応 OS（SafeOS）をベースにし、本研究サブテーマである、安全コンセプトおよび防衛機能の研究成果を SafeOS に追加する。この結果、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が実現する。

１－２　研究体制

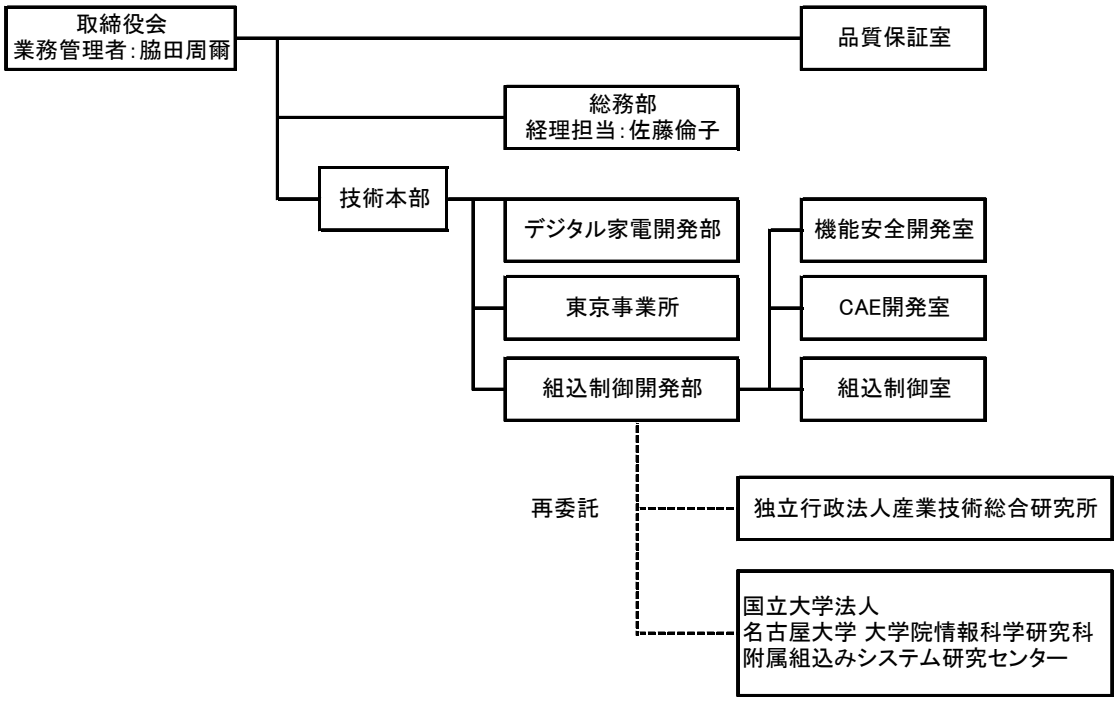


研究組織（全体）

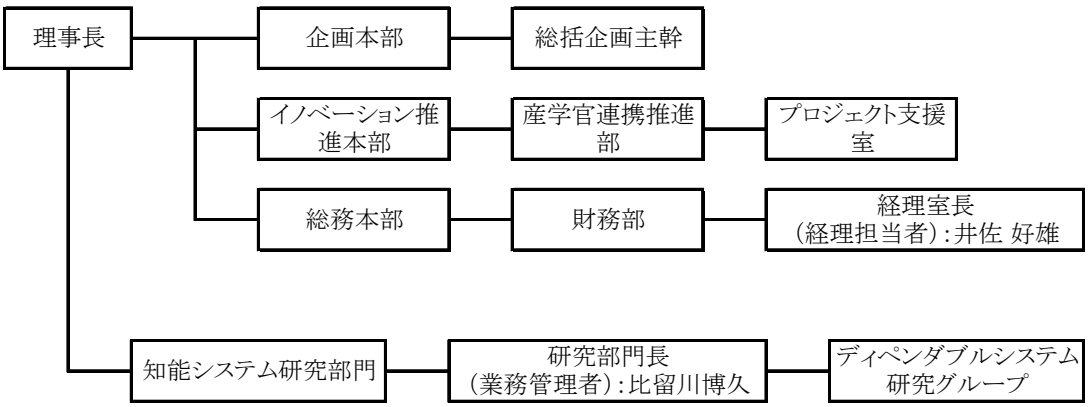


総括研究代表者（ＰＬ）	副総括研究代表者（ＳＬ）
株式会社ヴィッツ 常務取締役　組込制御開発部部長 服部　博行	国立大学法人名古屋大学 大学院情報科学研究科 附属組込みシステム研究センター 准教授　本田　晋也

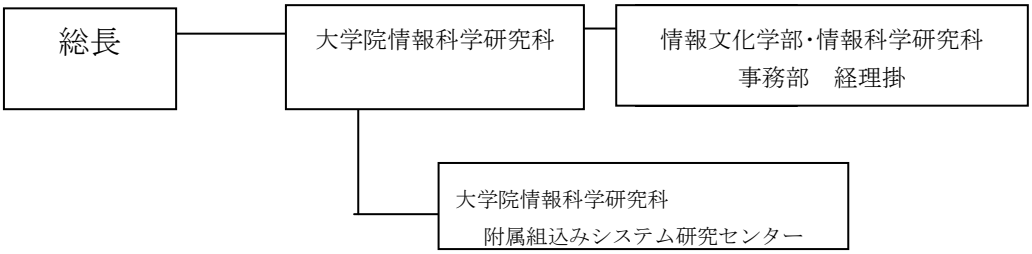
管理体制
①事業管理者
株式会社ヴィッツ



②（再委託先）
独立行政法人産業技術総合研究所



国立大学法人名古屋大学 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



管理員及び研究員

【事業管理機関】株式会社ヴィッツ

管理員

氏　名	所属・役職
安場尚一	会長
佐藤倫子	総務部　グループリーダ
岩瀬可奈	総務部
伊藤朋恵	総務部

研究員

氏　名	所属・役職
服部博行	常務取締役
森川聡久	組込制御開発部　機能安全開発室　室長
泉　明宏	組込制御開発部　機能安全開発室
片岡　歩	組込制御開発部　組込制御室　室長
吉田健太郎	組込制御開発部　組込制御室
杉山　歩	組込制御開発部　組込制御室
原　浩晃	組込制御開発部　機能安全開発室
松山貴之	組込制御開発部　機能安全開発室
加納かおり	組込制御開発部　組込制御室
吉田道信	組込制御開発部　機能安全開発室
戸澤　充	組込制御開発部　組込制御室
飯田義信	組込制御開発部　組込制御室
高橋明日香	組込制御開発部　機能安全開発室

【再委託先】

研究員

独立行政法人産業技術総合研究所

氏　名	所属・役職
水口大知	知能システム研究部門ディペンダブルシステム研究グループ・研究員
中坊嘉宏	知能システム研究部門ディペンダブルシステム研究グループ・主任研究員
安藤慶昭	知能システム研究部門統合知能研究グループ・主任研究員
藤原清司	知能システム研究部門 ディペンダブルシステム研究グループ・主任研究員
大場光太郎	知能システム研究部門・研究副部門長

国立大学法人名古屋大学 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

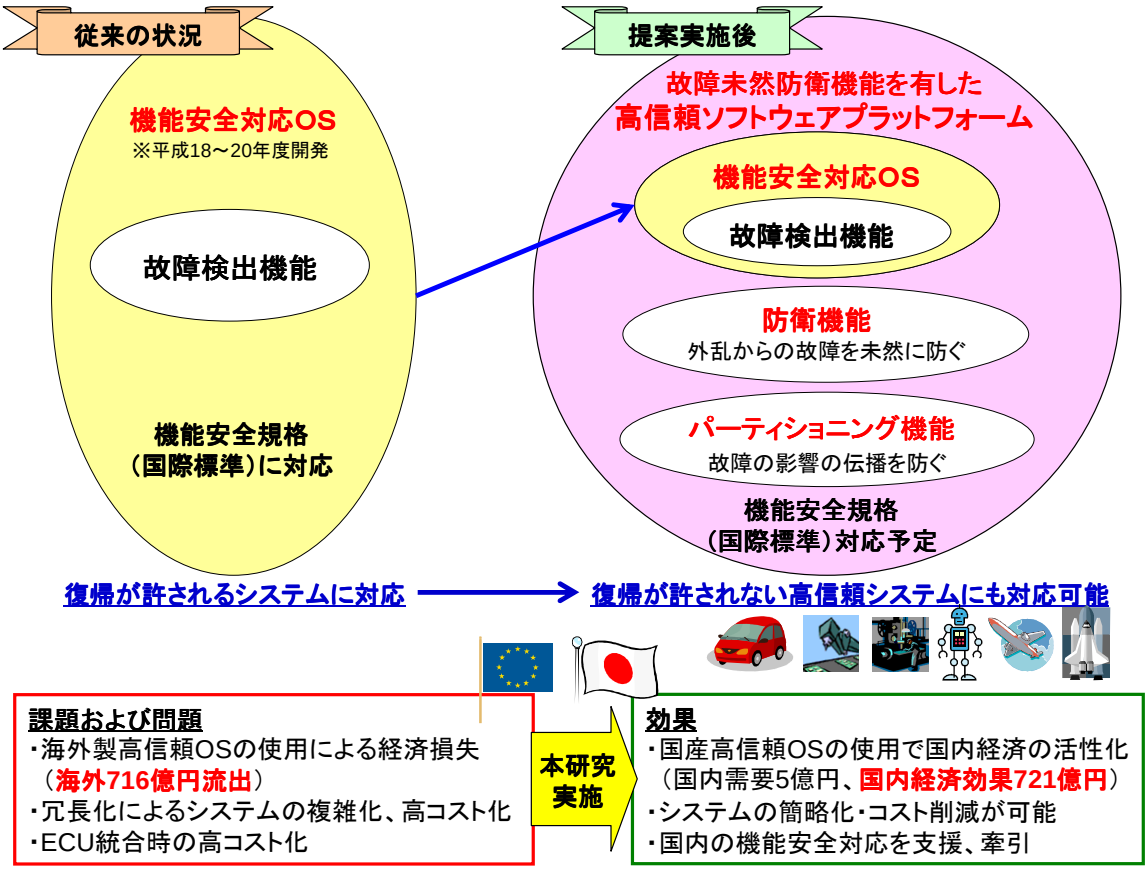
氏　名	所属・役職
本田晋也	大学院情報科学研究科 附属組込みシステム研究センター・准教授
高田広章	大学院情報科学研究科 附属組込みシステム研究センター・教授

アドバイザー

会社	部署	役職	氏名
トヨタ自動車（株）	パートナーロボット部 製品設計室　システム G	グループ長	山田　耕嗣
アイシン精機（株）	ソフトウェアセンター	主査	鈴村 延保
(株) 東海理化	エレクトロニクス機器事業部 エレクトロニクス技術部 制御システム開発室	室長	伊藤　茂二
オークマ（株）	FA システム本部 ソフト製品部	部長	深谷 安司
(株) デジタル	イノベーション＆IP 部 イノベーション＆コア開発グループ	マネージャー	杉岡 康次

1－3 成果概要

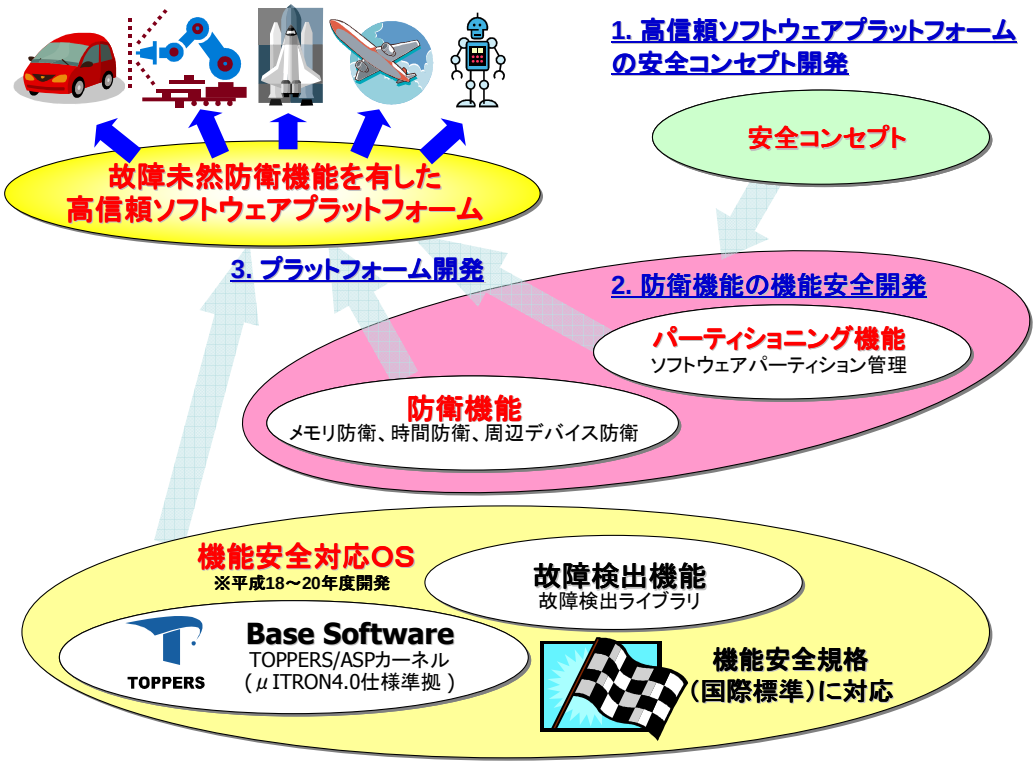
本研究の研究開発の全体図を以下に示す。



本研究を実施する名古屋大学と株式会社ヴィッツは、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**している。この研究成果では、**復帰が許されるシステムには対応できる**が、**復帰が許されない高信頼システム**（高度に電子制御された次世代自動車、サービスロボット、産業機械および産業ロボット、航空宇宙など）**への適応は困難**である。このため、**外乱からの故障を未然に防ぐ「防衛機能」**と、**万が一故障が発生しても故障**

の影響の伝播を防ぐ「パーティショニング機能」により、**強固な安全性を確保**し、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を開発する。

このような防衛機能を有する**国産の高信頼プラットフォームの開発は成功していない**が、本研究では 2000 万円程度での供給を目論んでいる。一方、**海外製の同種プラットフォームはいくつか存在**し、代表的な製品は導入に 1 社あたり数千万円程度、さらに別途ロイヤリティの費用が必要であり、**高価**である（**700 億円以上の海外流出**と予想）。



1. 高信頼ソフトウェアプラットフォームの安全コンセプト開発

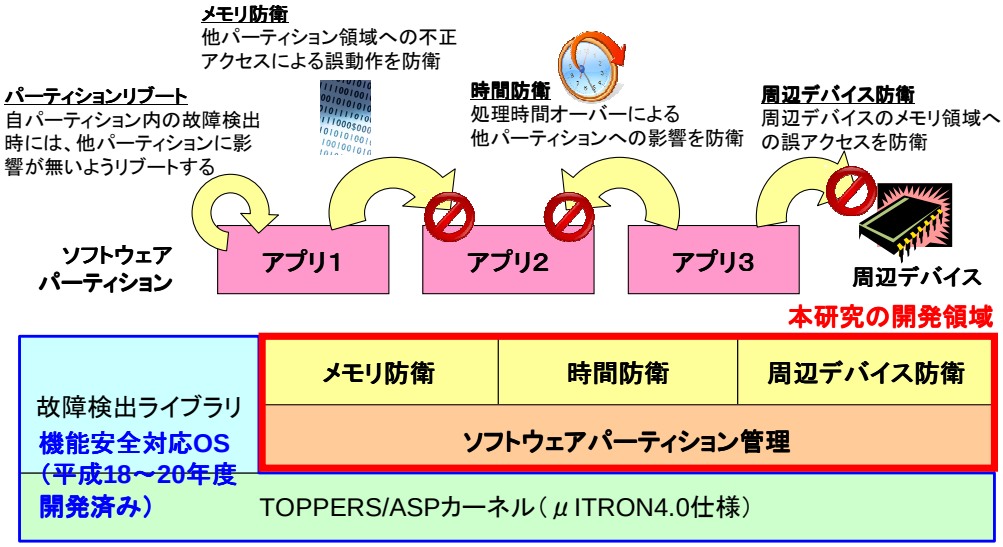
機能安全対応には安全コンセプトが正しく既定され、あらゆる状況において安全を担保する対策が施されている必要がある。この安全コンセプトの妥当性は、一般的に国際認証機関と協議をし、安全コンセプトを既定する。

2. 防衛機能の機能安全開発

外乱からの不正処理（故障）を防衛する機能を開発する。防衛機能として 1. メモリ防衛機能, 2. 時間防衛機能, 3. 周辺デバイス防衛機能, 4. パーティションのリブート機能 を開発し、これらの機能を総合して防衛を目的としたパーティショニング機能とする。

3. プラットフォーム開発

平成 18 年度 戦略的基盤技術高度化支援事業「機能安全対応自動車制御用プラットフォームの開発」にて開発した機能安全 OS (SafeOS) をベースプラットフォームとし、サブテーマ 2 にて開発した防衛機能を統合する。



【開発サブテーマと成果報告】

研究開発サブテーマの実施計画年度と研究成果等報告書概要版記載章番号の対応を以下に示す

開発サブテーマ	章番号	H22年度	H23年度	H24年度
高信頼ソフトウェアプラットフォームの安全コンセプト	2-1章	○	※1	※1
高信頼ソフトウェアプラットフォームの安全分析	2-1-1,2章	○	※1	※1
防衛機能検討	2-1-3,4章	○	○	—
安全コンセプト開発	2-1-5,6章	○	○	—
防衛率の定義と算出方法の検討	2-1-7,8章	○	○	—
防衛機能の機能安全開発	2-2章	—	○	○
メモリ防衛機能開発	2-2-1,2章	—	○	○
時間防衛機能開発	2-2-3,4章	—	○	○
周辺デバイス防衛機能開発	2-2-5,6章	—	○	○
パーティションリブート機能開発	2-2-7,8章	—	○	○
プラットフォーム開発	2-3章	○	—	○
ベースプラットフォーム開発	2-3-1,2章	○	—	—
故障未然防止高信頼プラットフォーム開発	2-3-3,4章	—	—	○
海外調査	2-4章	○	○	○
プロジェクトの管理運営	2-5章	○	○	○

１－４ 当該研究開発の連絡窓口

株式会社ヴィッツ
常務取締役　技術本部　組込制御開発部　部長　服部博行
TEL：052-223-7570　FAX：052-218-5855
E-mail：hat@witz-inc.co.jp

第2章　本論

２－１ 高信頼ソフトウェアプラットフォームの安全コンセプト

【概要】
本テーマでは、高信頼ソフトウェアプラットフォームが実現する安全目標を明確にし、高信頼性確保の方策（安全コンセプト）を策定した。策定した安全コンセプトを国際認証機関によるレビューを通し確立した。
また、高信頼ソフトウェアプラットフォームの安全コンセプトを確立するために、ソフトウェアプラットフォームの安全分析を実施し、機能安全規格には規定されていない、必要となる防衛機能の抽出と目標防衛率の計算手法や実現手段などを検討した。最後にその検討結果を安全コンセプトとしてまとめた。

２－１－１ 高信頼ソフトウェアプラットフォームの安全分析

復帰が許されない高信頼システムに必要な安全機能・防衛機能を導出するための安全分析を実施する。実施方法として、高信頼システム研究分野や高信頼システム開発で利用されている FTA, FMEA, HAZOP 分析を利用した。
この分析により、高信頼ソフトウェアプラットフォームに内在する障害項目の抽出、安全対策の規定、故障検出機能、防衛機能を導出し、安全分析シートとして取りまとめた。
本項目で得られた成果は、「防衛機能検討」, 「安全コンセプト開発」にて具体的な高信頼ソフトウェアプラットフォームの仕様やコンセプト策定に利用した。

２－１－２ 高信頼ソフトウェアプラットフォームの安全分析研究成果

高信頼ソフトウェアプラットフォームの安全分析を行い、その結果である安全分析シートを国際認証機関である TUV SUD にレビューを依頼し、安全分析結果が、国際的なレベルにおいて、十分かつ詳細であることを確認した。

２－１－３ 防衛機能検討

「実施内容１：高信頼ソフトウェアプラットフォームの安全分析」 にて実施した安全分析結果をもとに、故障未然防衛機能として有用な防衛機能仕様を検討し、防衛機能仕様を策定した。

防衛機能として、現時点ではメモリ防衛機能、時間防衛機能、周辺デバイス防衛機能、パーティションリブート機能は必須とするが、安全分析結果より更なる防衛機能を抽出した場合には追加し、故障未然防衛機能仕様として取りまとめた。
また、これら防衛機能の実現方法を検討するにあたり、マイクロコンピュータが有する機能への依存性とマイクロコンピュータへの新機能追加が考えられるため、防衛機能が発揮できる最適な開発機材の選定を行なった。選定された開発機材（マイコンボードやチップ開発キット）を用いマイクロコンピュータへの追加機能も同時に検討した。さらに、マイクロコンピュータに依存する機能の整理、マイクロコンピュータへの新規追加機能を整理した。

２－１－４ 防衛機能検討研究成果

メモリ防衛機能、時間保護防衛機能、パーティションリブート機能、周辺デバイス防衛機能の各機能仕様について策定を行い、国際認証機関からの技術評価を受け、防衛機能として有益である事を確認することができた。

さらに、開発・性能評価を行なった結果を踏まえて、アドバイザが求める性能要求を達成できるよう改善した低リソース・高応答性な防衛機能仕様（BCC+）を追加策定し、これについても国際認証機関からの技術評価を受けることができた。

また、本研究成果を有効活用するため、本研究成果であるハードウェア要件を特許として出願し（特願2012-228375)、広く世の中にアピールすることとした。

２－１－５ 安全コンセプト開発

「２－１　高信頼ソフトウェアプラットフォームの安全分析」 にて実施した安全分析結果をもとに、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安全コンセプトを策定した。

高信頼ソフトウェアを開発するには、国際安全規格である機能安全規格（IEC 61508）への準拠が必要と考えた。第三者による機能安全規格への適合認証には、安全コンセプトの国際認証機関（第三者）との合意が不可欠である。そのため本研究では、国際認証機関であるドイツ TUV SUD に安全コンセプトのレビューを依頼(TUV SUD により安全コンセプトレポートとして取りまとめられる）し、問題事項・改修指摘事項・追加項目などを明確にし、安全コンセプト仕様として取りまとめた。

機能安全ソフトウェア開発プロセス認証を取得している株式会社ヴィッツの安全 OS における安全コンセプト開発経験と、国立大学法人名古屋大学の先進的なプラットフォーム知識や研究実績から安全コンセプトの策定を行なった。通常、国際認証機関との安全コンセプト合意には 20 日程度のディスカッションを要すると見込まれるが、国内で模擬的な検討活動を実施することによりディスカッション日時を短縮した。すなわち、株式会社ヴィッツが機能安全ソフトウェア開発プロセス認証取得時に模擬的な認証アセスメントを実施した経験を持つ独立行政法人産業技術総合研究所が模擬的な認証を行うことにより、効率的に進めることができた。

２－１－６ 安全コンセプト開発研究成果

3 年間の研究を通して、高信頼ソフトウェアプラットフォームについて、低リソース・高応答性対応した仕様の策定を行い、最終仕様についての安全コンセプトを策定することができた。

さらに、認証機関による技術レビューにより、最終コンセプトレポートを取得することができ、機能安全 IEC61508 SIL3 で求められる安全性を満たすことが、外部機関により証明された。

２－１－７ 防衛率の定義と算出方法の検討

本研究では、IEC 61508 が規定する故障検出機能に加えて、ソフトウェア故障に関する防衛機能を充実させるため、防衛機能を評価するのに相応しい指標について検討し、導入を図った。

また、メモリ防衛機能や時間防衛機能等の防衛機能を評価するための指標として「防衛率」を定義し、定義した防衛率を用いて、高信頼ソフトウェアプラットフォームの防衛機能を評価した。さらに、「パーティションレベル」の定義も実施した。

表2-1-7-1　パーティションレベル

防衛機能	パーティションレベル1	パーティションレベル2	パーティションレベル3	パーティションレベル4

サービス保護	○	○	○	○
メモリ保護	○	○	○	○
CPU利用率保護		○	○	○
実行シーケンス保護			○	○
実行タイミング保護				○

２－１－８ 防衛率の定義と算出方法の検討研究成果

防衛率の定義と算出方法について検討した結果についてTUV SUDと議論し、「パーティションレベル」を定義することで、防衛率に相当する役割を果たすものになる、という結論を得ることができた。

２－２ 防衛機能の機能安全開発

【概要】

外乱からの不正処理（故障）を防衛する機能を開発する。防衛機能として 1. メモリ防衛機能, 2. 時間防衛機能, 3. 周辺デバイス防衛機能, 4. パーティションのリブート機能 を開発し、これらの機能を総合して防衛を目的としたパーティショニング機能とした。

そのため、高信頼ソフトウェアプラットフォームに必要な防衛機能仕様の策定とそのソフトウェア開発を行なった。

尚、ソフトウェア開発は機能安全 IEC61508 SIL3 相当のソフトウェア開発プロセスにて実施する必要がある。株式会社ヴィッツは2010年4月に、機能安全国際認証機関であるTUV SUD (Germany) から“日本初の機能安全プロセス認証”を取得しているため、防衛機能の機能安全開発は問題なく実施可能であった。

２－２－１ メモリ防衛機能開発

プロセッサに搭載されたMPU (Memory Protection Unit) を用い、リアルタイム特性を維持したままのメモリ防衛機能を実現した。MPUを用いたメモリ防衛の基本機能は、平成17年度「自動車統合制御用組込みOSの開発」において、提案者らにより実現している。この研究成果をベースとして、機能安全対応に必要な機能を追加し、さらに機能安全開発プロセスを適用したメモリ防衛機能を実現した。

２－２－２ メモリ防衛機能開発研究成果

高信頼ソフトウェアプラットフォームにおけるメモリ防衛機能について、当初計画していた開発を完了することが出来た。高信頼ソフトウェアプラットフォーム全体としては、アドバイザが求める性能要求を満たせていない課題があるが、メモリ防衛機能単体としては性能評価結果も妥当と判断しており、当初計画していた機能の開発が完了したと判断している。

２－２－３ 時間防衛機能開発

階層型スケジューラ方式を利用した時間防衛機能の開発を実施した。階層型スケジューラによる時間防衛機能も提案者らにより既に基本機能は実現している。本研究では、先の研究成果を基本仕様とし、航空宇宙で利用されているスケジューラ（PikeOSなど）との比較調査を行い、最下層スケジューラを改良について検討した。すなわち、先の研究では、ECU統合を容易にすることを目的として研究したが、本研究では機能安全側面に立ち、処理間の独立性を高め、時間的干渉や時間的障害防衛を強化した階層型スケジューラを開発した。

２－２－４ 時間防衛機能開発研究成果

高信頼ソフトウェアプラットフォームにおける時間防衛機能について、当初計画していた開発を完了することが出来た。また、高信頼ソフトウェアプラットフォーム全体としてアドバイザが求める性能要求を満たせていない課題があったため、性能改善活動を追加実施することが出来た。

２－２－５ 周辺デバイス防衛機能開発

高信頼ソフトウェアプラットフォームを実現するには、周辺デバイスの監視と保護も必要になる。提案者らがECU統合を目的に開発した防衛機能では、プロセッサのレジスタ監視とその動作による防衛は実現できているが、レジスタ等を利用せずにメモリにアクセスできるデバイスなどは防衛対象にはなっていない。すなわち、DMAコントローラなどバスに直接つながり動作するデバイスの防衛は実現できていない。しかし、高信頼ソフトウェアプラットフォームにはメモリにダイレクトにアクセスしている周辺デバイスからのメモリ防衛は必須と考えられ、これらの周辺デバイスからの不正処理を防衛する機能の実現に取り組んだ。

尚、本機能実現にあたり、検討したデバイスの他に干渉する恐れが無いことを証明するのは困難な問題となることが予想されたため、これらの課題対策はハードウェアメーカおよび認証機関等の知識を取り入れて対処した。

周辺デバイス防衛機能を実現するために、以下に示す研究を実施した。

実施内容:「ハードウェアへの要求事項の検討」

周辺デバイス防衛機能は、既存のアクセス保護技術であるTrustZoneを拡張することで実現する。具体的には、以下の２項目について機能拡張を行なった。

- 複数のパーティションからのアクセス許可・禁止を管理するため、既存のTrustZoneでは1bitで管理されているアクセス許可・禁止情報を、複数bitで管理するように拡張した。
- マスタデバイスが不正（他パーティション動作中）にバス帯域を利用することから保護するために、バスコントローラに対してアクセス権を確認する機能を追加拡張した。

これらの機能拡張は、どちらもハードウェアの改造が必須であった。改造の概要を以下に示す。

- 現在の状態を示す1bitの情報（Secure/NonSecure）を、現在の実行パーティションを示す複数bitの情報（パーティション識別子）に拡張した。
- 現在動作しているマスタデバイスのアクセス権を示す1bitの情報（Secure/NonSecure）を、マスタデバイスが所属するパーティションを示す複数bitの情報（パーティション識別子）に拡張した。
- スレーブデバイスのアクセス権を示す1bitの情報（Secure/NonSecure）を、スレーブデバイスが所属するパーティションを示す複数bitの情報（パーティション識別子）に拡張した。
- バスコントローラは、現在の実行パーティションの情報とバスアクセスを試みるマスタデバイスが所属するパーティションの情報から、バスアクセスの許可・禁止を判断する。
- スレーブデバイスは、現在の実行パーティションの情報とデバイスアクセスを試みるマスタデバイスが所属するパーティションの情報から、デバイスアクセスの許可・禁止を判断する。

２－２－６ 周辺デバイス防衛機能開発研究成果

高信頼ソフトウェアプラットフォームにおける周辺デバイス防衛機能について、ハードウェアへの要求事項の導出を行なった。なお、前記要求事項を満足するハードウェアは調査した限り国内外を通じて存在しておらず、周辺デバイス防衛機能を実装開発するための実装環境を入手することが困難である。このため、ハードウェアへの要求事項の導出と特許出願をもって、本研究項目を完了した。

２－２－７ パーティションリブート機能開発

防衛機能は多種多様な障害を事前に防衛し、障害を発生しない、もしくは拡大しないための機能である。パーティショニングは前述機能と連携して、個別の機能単位を分離し、他への波及を防ぐものであるが、万が一障害を発生した場合には、機能単位で障害を検出し復帰させる機能が必要である。これをパーティションリブート機能として開発をおこなった。

この機能は、欧州発標準仕様であるAUTOSARでも仕様化されているが、AUTOSAR仕様は複雑すぎて、安全機能として利用するには難しい。そのため、AUTOSARが提案する仕様を実現することはもとより、さらにシンプルで同程度の機能を実現することを検討し開発を行なった。

パーティションリブート機能を実現するために，以下に示す2つの研究を実施した。

①:「パーティションの起動／終了処理と再起動処理の設計」

パーティションを個別にリブートするための機能を提供するため、パーティションの初期化処理／終了処理はパーティションに割り付けられたタイムウィンドウ内にて実行を行う。

②:「簡易性能評価の実施」

パーティションリブート機能として追加されたAPIの処理時間の計測を行なった。具体的には、APIの開始時刻と終了時刻を計測し、APIの処理時間とした。

パーティションリブート機能を改善するために、以下に示す2つの研究を実施した。

①：「パーティションリブート機能の改善方針の検討」

アドバイザが求める性能要求を満たすために、パーティションリブート機能に対してどのような改善を行うとよいか検討を行なった。具体的には、処理時間が長くかかっている機能および仕様を分析し、過剰な機能を削減することで処理性能の向上を狙った。システム全体として処理時間が長く過剰な機能と判断したのは以下2つの機能である。

・システム割り込み
・アイドル属性パーティション

②:「パーティション初期化処理簡素化」

ECCではシステム周期が開始されると、まずシステムパーティションの起動が行われ、システムパーティションとして実行する処理がない場合、システムパーティションがアイドル状態となり、アプリケーションパーティションが起動するという流れとなる。BCC+にてシステムパーティションの概念をなくしたことで、パーティション初期化時のパーティション切替え処理を削除できる。

２－２－８ パーティションリブート機能開発研究成果

高信頼ソフトウェアプラットフォームにおけるパーティションリブート機能について、当初計画していた開発を完了することが出来た。また、高信頼ソフトウェアプラットフォーム全体としてアドバイザが求める性能要求を満たせていない課題があったため、性能改善活動を追加実施することが出来た。

２－３ プラットフォーム開発

【概要】

高信頼システムで利用可能な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を開発する。開発済みであるSafeOSをベースとして、目標とする故障率の達成や防衛率を実現するために、機能追加および改良を加える方法で、ソフトウェアプラットフォームの開発を進める。また、以下の手順で開発を行なった。

まず、目標の故障検出率を達成するために、IEC 61508の第2部で紹介されている以下の故障検出機能を故障検出ライブラリに追加開発した。

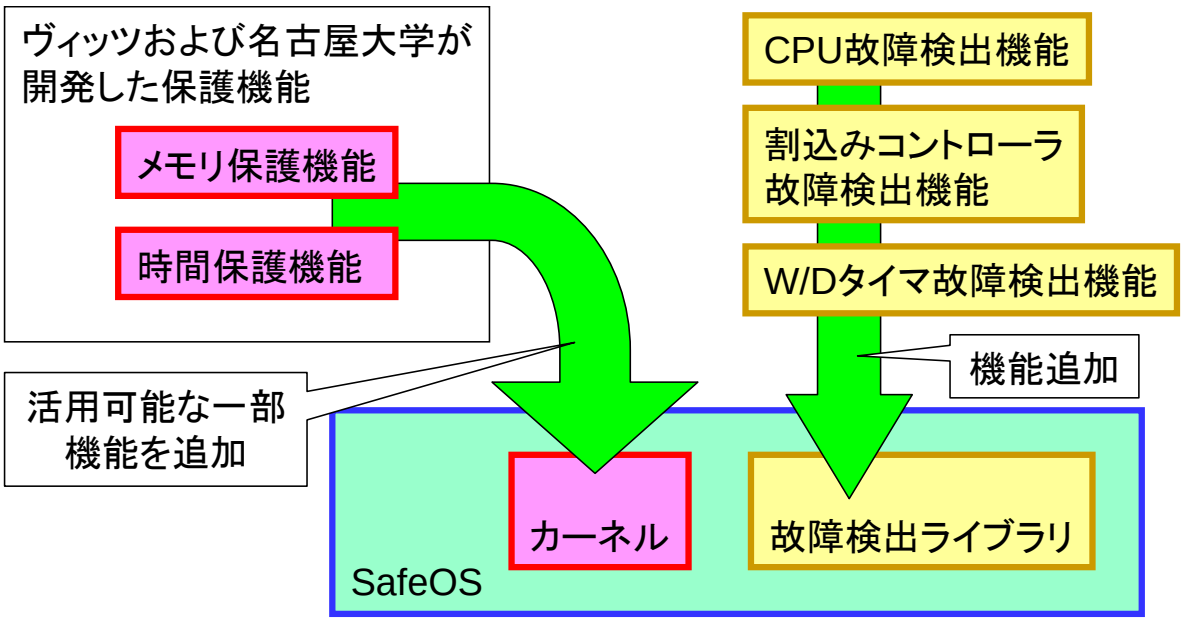
- CPU故障検出機能
- 割込みコントローラ故障検出機能

また、SafeOSのSafety Conceptにて検討されている以下の機能を、故障検出ライブラリに追加開発した。

- W/Dタイマ故障検出機能

次に、株式会社ヴィッツおよび国立大学法人名古屋大学が開発したメモリ保護機能、時間保護機能について、故障未然防止高信頼プラットフォームの防衛機能として活用可能な部位を特定し、カーネル機能として追加開発をした。

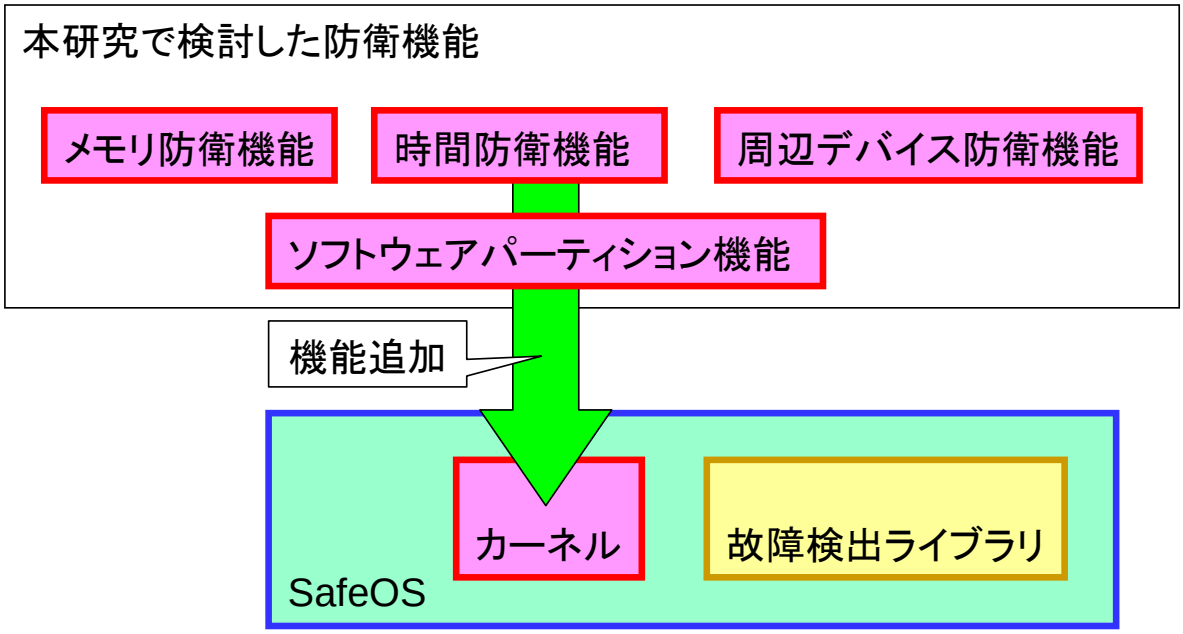
これらの機能をベースとするソフトウェアプラットフォームに追加開発することで、ベースプラットフォームの育成開発を行なった。



ベースプラットフォームの開発イメージ

最後に、目標の防衛率を実現するために、前述の通り検討を行なっている以下の機能を追加開発し、故障未然防止高信頼プラットフォームを開発した。

- メモリ防衛機能
- 時間防衛機能
- 周辺デバイス防衛機能
- ソフトウェアパーティション機能



故障未然防止高信頼プラットフォームの開発イメージ

なお、これら全ての開発は、機能安全 IEC61508 SIL3 相当のソフトウェア開発プロセスにて行なう必要がある。

2－3－1　ベースプラットフォーム開発

故障未然防止高信頼プラットフォームのベースとなるソフトウェアプラットフォームを開発する。

①:故障検出ライブラリに、CPU故障検出機能、割込みコントローラ故障検出機能、W/Dタイマ故障検出機能を追加開発した。開発はFSMPに記載されているV字プロセスに従って実施した。

②メモリ保護機能と時間保護機能について、活用可能な部位の検討を行なった。
検討は、各保護機能の機能仕様書と、防衛機能のコンセプトを比較することで実施した。比較項目は各保後機能の詳細機能とし、防衛機能のコンセプトを実現する機能として流用可能か判断を行なった。

2－3－2　ベースプラットフォーム開発研究成果

予定していたCPU故障検出機能、割込みコントローラ故障検出機能、W/Dタイマ故障検出機能の追加開発が完了し、故障未然防止高信頼プラットフォームの開発を進めることが可能な状態となった。

2－3－3　故障未然防止高信頼プラットフォーム開発

「第3章　防衛機能の機能安全開発」にて開発した各種防衛機能と「4-1　ベースプラットフォーム開発」にて開発したプラットフォームベースを統合し、故障未然防止高信頼プラットフォームの開発を行なった。

①:ベースプラットフォームと、メモリ防衛機能、時間防衛機能、パーティションリブート機能を統合し、高信頼ソフトウェアプラットフォームを開発した。また、開発した高信頼ソフトウェアプラットフォームに対して、アプリケーションを想定した負荷をかけた状態での、性能評価を実施した。機能の統合については特記すべき事項が無いため、性能評価概要についてのみ記載した。

②:性能評価の結果、アドバイザが求める性能要求を満たせていないという課題が定義された。これに対し、各防衛機能にて対策の検討を行い、その結果をBCC+仕様にまとめた。高信頼ソフトウェアプラットフォームのBCC+仕様を実現するための設計を行なった。

③:平成23年度に検討していたWD付実行シーケンスモニタでは、アプリケーションシーケンスモニタと、タイムウィンドウシーケンスモニタが独立しているため、WDタイマがそれぞれ必要であると判断していた。しかし、WDタイマを2つ搭載しなければならないというHW制約はコストに対する影響が大きいと考え、1つのWDタイマで２つのシーケンスモニタを行う手法の検討を行なった。

２－３－４ 故障未然防止高信頼プラットフォーム開発研究成果

高信頼ソフトウェアプラットフォームについて、各機能の統合および性能評価を実施し、当初計画していた開発を完了することが出来た。なお、高信頼ソフトウェアプラットフォーム全体としてアドバイザが求める性能要求を満たせていない課題があったため、性能改善活動を追加実施したが、仕様検討および再設計を行なったところで研究期間を満了した。

このため、管理法人と研究機関が継続研究の実施を妥結し、継続研究にて残課題である機能の実装と評価を実施・完了する計画である。

２－４海外調査

【概要】

高信頼ソフトウェアプラットフォームは、プラットフォーム上で稼動する各種アプリケーションの故障を伝播させない機能を有するプラットフォームである。そのため、高信頼ソフトウェアプラットフォーム自体が安全設計されていなければならない。

ソフトウェアの安全設計の規格として、機能安全 IEC 61508 がある。研究母体である株式会社ヴィッツは国内唯一の機能安全 IEC 61508 SIL3 プロセス認証を取得している企業であり、認証取得企業が認証プロセスに従い開発したソフトウェアは安全設計がされ、高信頼ソフトウェアプラットフォームが必要な安全性を兼ね備えるといえる。

しかし、ソフトウェアを安全に設計したとしても、安全を得るためのコンセプトが正しく規定されていないと意味がない。また、そのコンセプトが国際的な標準と比較し、遜色ないことが必要である。

そこで、本研究では、機能安全の国際認証期間である TUV SUD に機能安全コンセプトフェーズのレポートを入手し、本研究で開発する安全コンセプトが妥当であることを確認して、研究成果である高信頼ソフトウェアプラットフォームを開発した。

２－４－１ 安全コンセプトの認証機関レビュー

機能安全規格では、設計初期段階で安全性を如何に確保するかの安全コンセプトが定まっていることが要求されている。そのため、国際認証機関から認証を取得するためには、認証機関によるコンセプトのレビューレポートが必要となる。

本研究では、製品認証を取得するだけの費用が捻出できないことと、研究予算を認証費用として支出できないことから、認証取得は研究終了後の事業化にて検討した。

本研究では、コンセプトフェーズのコンセプトレポートを取得し、かつ、開発成果の監査レビューを取得を目指した。
尚、上記のレポートは認証を取得するためには必要なステップであり、通常の製品認証においては、上記のレポートに加え、各種の試験が実施され、製品認証取得となる。

① 平成22年11月末に「高信頼ソフトウェアプラットフォームの安全コンセプト開発」にて開発した以下の文書のドキュメントレビューを国際認証機関 TUV SUD に依頼した。
＜技術ミーティング＞
平成23年1月10,12,14日に国際認証機関TUV SUD と技術ミーティングを実施した。

②平成23年8月末に「高信頼ソフトウェアプラットフォームの安全コンセプト開発」にて開発した以下の文書のドキュメントレビューを国際認証機関 TUV SUD に依頼した。いずれも、前年度のレビューにおける指摘事項を反映したものである。
＜ドキュメントレビュー＞
コンセプトレポートのためのレビュー対象文書

No	Title	Document-No./ File identifier	Revision	Date
[D1]	Reliable OS Safety Concept	SafetyConcept_E.doc	0.3	24.9.2011
[D2]	Software Safety Requirement Specifications	SoftwareSafetyRequirementSpecification.doc	0.30	24.9.2011
[D3]	Reliable OS Safety Manual	SafetyManual.doc	0.30	6.10.2011
[D4]	Safety Analysis	SafetyAnalysis.xls	0.02	31.10.2011

ドキュメント番号[D1]から[D4] は、事前に英訳し、送付した資料である。
＜技術ミーティング＞
平成23年9月12、14、16日に国際認証機関TUV SUD と技術ミーティングを実施した。

③平成24年8月末に「高信頼ソフトウェアプラットフォームの安全コンセプト開発」にて開発した以下の文書のドキュメントレビューを国際認証機関 TUV SUD に依頼した。いずれも、前年度のレビューにおける指摘事項を反映したものである。
＜ドキュメントレビュー＞
コンセプトレポートのためのレビュー対象文書

No	Title	Document-No./ File identifier	Revision	Date
[U1]	Software Safety Requirement Specification	ParOS-SW-01-REQ	0.61	2012-Sep-19 DRAFT
[U2]	Confirm Corresponding Plan to TUV Report in Safety Analysis	ConfirmCorresponding-PlanToTUVReportInSafetyAnalysis.ppt	---	2012-July-03
[U3]	Partition OS Safety Concept (E)	SafetyConcept_E.doc	0.61	2012-Sep-19 DRAFT
[U4]	Safety Manual	SafetyManual_E.doc ParOS-SW-01-SM	0.62	2012-Sep-22 DRAFT
[U5]	Partition OS Safety Requirements Analysis Plan and Results Report	PartOS_SafetyRequirementsAnalysisPlanAndResultsReport.doc ParOS-SW-01-SA	0.03	2012-Sep-21 DRAFT

		ParOS_SafetyRequirementAnalysisResultReport(detail).xls	0.05	2012-Sep-21 DRAFT

＜技術ミーティング＞
平成24年9月18、19、21日に国際認証機関TUV SUD と技術ミーティングを実施した。

２－４－２ 安全コンセプトの認証機関レビュー研究成果

平成22年度の海外調査は予定していたテクニカルレポートを得て完了した。テクニカルレポートで指摘された、問題事項、推奨対応方法などを検討し、プラットフォーム仕様に反映した。
平成23年度の海外調査は、コンセプトフェーズ文書のレビューを受けて完了した。指摘事項を反映した文書はTUV SUDへ再提出し、テクニカルレポートを取得している。
平成24年度の海外調査では、安全コンセプト、安全要求仕様書、および、安全マニュアルについては、ミーティング直後までにすべての指摘事項をクローズすることができた。安全分析結果については、上記の３つの観点で指摘事項が残ることとなったが、ミーティング終了までにそれらの対応策を合意することができた。そのため帰国後の対応にて、すべての指摘事項をクローズすることができており、安全上問題ないというテクニカルレポートを最終的に受領できた。

２－５ プロジェクトの管理・運営

【実施内容概要】
当該研究を適切且つ効果的に実施するために、本プロジェクトでは、プロジェクト進捗管理を目的とした会議（研究開発委員会）および研究の技術的解決を図る会議（技術検討委員会）を定期的に実施してプロジェクトの管理を行う。
また、上記で記載したプロジェクト全体での管理・運営の他に、研究実施者を専門の複数のグループに分割し、個別のグループ検討会議を実施するなど技術的に深い検討を重ねて、プロジェクトの技術的な進捗および運営を行う。

２－５－１ 研究開発委員会成果

3年間を通じて、2ヶ月に一度進捗管理を目的とした研究開発委員会を実施し、各開発においてスケジュール的な問題や成果方針などの決定・指示を行うことができた。研究期間を通じ、良好な運営を行なうことができた。
また、PLは主に事業化・運営に責任をもち、SLが技術的な責任を持つなどの職務分掌が出来ており、各プロジェクトで問題等が発生した時に、速やかに対処することができた。
以上により、実施計画書に記載していた目標のすべてを達成することができた。

２－５－２ 技術検討委員会成果

技術検討委員会を通じ、技術的な課題を解決した。また、アドバイザ各位から、当該業界の現状、高信頼プラットフォームへの要望事項、安全対策、製品適用性、コストイメージ等のアドバイスをいただき、仕様策定に取り入れられたことは大きな成果であると考える。

最終章　全体総括

本研究は自動車・産業ロボット・生活支援ロボット・航空宇宙などが必要とする、安全性を確保し、かつ、万が一故障が発生してもその故障を伝播させない機構(機能維持) を併せ持つソフトウェアプラットフォームの研究である。3年間の研究を通じ、当初目標である安全性を兼ね備えた堅牢なソフトウェアプラットフォームを完成させた。

本研究成果であるソフトウェアプラットフォームは、自動車向け標準仕様である AUTOSAR を参考にし、さらに、航空宇宙で利用されている ARINC 653 仕様をベースにしたプラットフォームであり、パーティショニング機能を活用した安全性の高いプラットフォームである。

一方、提案申請時には防衛率の策定を検討していたが、国際認証機関とのテクニカルディスカッション等により、新たな規格(Standard) を策定することは容易ではないため、複数の防衛基準を策定し防衛基準に合致したソフトウェアプラットフォームを開発するのが事業化においても重要だと判断した。そのため本研究途中より、複数のコンフォーマンスクラスを策定し、その最も防衛機能が高いコンフォーマンスクラス(ECC) のプラットフォームの開発を完了している。さらに、防衛機能が低いものの、軽快に動作するコンフォーマンスクラス (BCC+) の開発にも着手し、幅広く組込み機器に利用できる道筋を構築している。

これら開発成果物の技術的なポイントとして、国際認証機関から安全コンセプトに関するコンセプトレポートを取得し、国際的な技術水準を担保している証拠の取得にも成功した。

これら開発成果より、本研究は当初予定以上の技術成果を得ることができ、かつ、事業化にも積極的な取り組みを行い、すでに国内大手企業が試作に利用開始するなど実用化にも着手できている。