18-12

平成２０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」

研究開発成果等報告書

平成２１年１１月

委託者　　独立行政法人中小企業基盤整備機構

委託先　　株式会社ヴィッツ

目　　次

第１章　研究開発の概要

１．研究開発の背景・研究目的及び目標

(1)　研究の背景

自動車産業は日本を代表する産業であり、国内メーカは世界一の生産台数を誇る重要産業である。さらに、生産される自動車の品質は世界一であり、生産台数及び品質においても世界一の地位を占め、非常に優れた技術を保持している産業である。このように諸外国をリードする産業においても、標準化および規格化など一部の分野では遅れが目立ち、欧米の規格化戦略の後塵を拝している。例えば、欧州の自動車メーカが中心となり策定された、自動車用 OS の OSEK/VDX OS や車載通信仕様 CAN, LIN, FlexRay などは国際的に利用が進み、国内自動車メーカは追従せざるをえない状況になりつつある。更に、2006 年 6 月末に AUTOSAR から、次世代の自動車用基本ソフトウェア等の国際標準を狙った仕様が公開されており、日本の標準化対策は大きく遅れをとった状況である。

さらに、規格安全においても、欧州の機能安全規格が世界規模で義務づけられつつあり、川下製造業者はこの機能安全にも対応する必要が生じ、高度化指針においても川下産業の課題として挙げられている。一方、安全について考えると、国内自動車は世界的にみても高い水準にあり、日本の自動車は世界で一番安全な自動車を開発・生産していると理解されている。このように高い安全水準を持った国内メーカが、日本より安全性レベルの低い欧州メーカの安全基準に合致させないといけないかは、大きな疑問であると言わざるを得ない。事実、国内自動車メーカの意見として、ユーザは現在の安全品質に満足しており、安全に対する対策が必要だと感じていないとの意見もある。このような日本の高い安全品質は日本のものづくりである、”摺り合わせ”により実現できた産物であるが、問題は日本の安全性・技術力を数値評価する方法が無いことである。一方、欧州は他民族・多言語文化であり、多言語文化で技術力の継承および安全を維持するには、ドキュメントによる継承および指針が有効である。さらに、欧州の自動車メーカは、機能安全規格により、安全性に関する取り組みが実施されつつあり、機能安全への対応で欧州の自動車の安全性が高まるメリットがある。

国内の安全性への取り組みに目を向けると、国内メーカは、「ぶつからない車」、「交通事故０」を目標として対策しており、欧州主導の機能安全を実施しても、自動車の安全性が向上するとは言い難いのが現状である。一方で次世代の自動車に利用されることが確実視されている X-by-Wire 技術は、車の基本機能を機械ではなく、電子化（ コンピュータと通信技術 ）で実現するものであり、この技術を用いた製品を開発・販売するためには、現在日本で考えている電子部品に対する安全だけではなく、安全を実現する手法や安全を証明できる手法が必要になると考えられる。そのため、国内メーカにおいても、現在の製品への機能安全対策は必ずしも重要であるとはいえないものの、次世代の自動車開発には“評価基準”という意味で重要となる。

そこで、国内メーカが機能安全対策の実施方法を考えると、機能安全規格を“そのまま、一字一句、全ての項目を”対策すると、安全認証コストはかさむが国内メーカが得られるものは少ない。この状況に陥ることは、欧州自動車メーカ、ひいては、欧州連合[1]の世界戦略手法に陥ることになる。そのため、国内の機能安全に対する取り組みとして、機能安全認証に必要な項目すべてを不足無く実施するのではなく、対応するべき項目の重要度、不足項目の追加などを提言し、かつ、欧州規格に日本のものづくりを提案して自動車業界全体としての安全性を確保できるように注力するのが望ましいと考える。そこで、国内自動車メーカが機能安全対策を必要とした時に、すでに対応された基盤ソフトウェアが存在することと、機能安全対策に必要な対応項目の選択および重要度を理解していることが重要となる。

(2) 研究の目的及び目標

基盤ソフトウェアの安全性能開発および機能安全対応可能企業育成を目標とする。

① 機能安全に対応した自動車制御用組込み OS の開発

国内初の機能安全（IEC61508 SIL-3）対応組込み OS の開発を成功させる。

さらに、当該製品の販売、サポート事業の立ち上げ、および機能安全対応可能な企業集団の擁立を実現する。

② 機能安全に対応した自動車用通信ミドルウェアと次世代車両用例示アプリケーションの開発

機能安全に対応した現世代車両通信（ CAN / LIN ）および次世代車両通信（FlexRay）の開発を成功させる。

また、本研究で開発する機能安全対応組込み OS および機能安全対応自動車用通信ミドルウェアを利用した例示アプリケーションの開発を成功させる。

２．研究体制

【実施内容】

研究開発項目
機能安全開発プロセスの規定
② 基本 OS に求める安全機能の開発
③ ソフトウェア安全分析およびコンポーネント手法
④ 機能安全対応自動車制御用組込み OS の開発
⑤ 機能安全対応 CAN 通信ミドルウェアの開発
⑥ 機能安全対応 LIN 通信ミドルウェアの開発
⑦ 機能安全対応 FlexRay 通信ミドルウェアの開発

1 欧州連合は、機能安全規格を策定するための費用として、5th Framework と EAST-EEA で合計 3,650 億円（およそ 5 年程度 ）を助成し、規格策定と同時に国際標準化も実現している

⑧　次世代例示アプリケーションの開発 ⑨　機能安全対象機器の開発 ⑩　開発過程のドキュメント作成および機能安全教育コンテンツの開発 ⑪　機能安全規格調査および機能安全対策調査 ⑫　プロジェクトの管理・運営 ⑬　コンピテンシ ⑭　機能安全監査と評価

(1)　管理体制

【管理法人】株式会社ヴィッツ

〒４６０－０００８　名古屋市中区栄二丁目 13 番 1 号白川第 2 ビル

氏　名	所属・役職	実施内容	備考
安場　尚一	会長	⑫	06.12～
脇田　周爾	代表取締役	⑫	06.12～
佐藤　倫子	総務部	⑫	06.12～
岩瀬　可奈	総務部	⑫	06.12～

総括研究代表者（ＰＬ） 国立大学法人名古屋大学　大学院情報科学研究科　教授　　高田 広章

副総括研究代表者（ＳＰＬ） 株式会社ヴィッツ　取締役　　服部 博行

(2)　研究体制

株式会社ヴィッツ

氏　名	所属・役職	実施内容	備考
服部博行	取締役兼組込制御開発部部長	①②③④⑤⑥⑦⑧⑨⑩⑪⑬⑭	06.12～
森川聡久	組込制御開発部　課長代理	①②③④⑧⑨⑩⑪⑬⑭	06.12～
丹家廉	組込制御開発部　課長代理	①②③④⑧⑨	07.3～
長江宣宗	組込制御開発部　研究員	①②③④⑤⑥⑦⑧⑨⑩⑪⑬⑭	07.3.～
鵜飼敬幸	組込制御開発部　副主査	①②③④⑤⑥⑦⑧⑨⑪	06.12～

		⑬⑭	
片岡　歩	組込制御開発部　副主査	①②③④⑤⑥⑦⑧⑨⑪⑬	06.12～
大西秀一	組込制御開発部　課長代理	①②③④⑧⑨⑪⑬	06.12～
安田友巳	組込制御開発部	①②③④⑤⑥⑦⑧⑨⑪⑬	06.12～08.11
水野智仁	組込制御開発部	①②③④⑤⑥⑦⑧⑨⑪⑬	06.12～
小川貴章	組込制御開発部	①②③④⑤⑥⑦⑧⑨	06.12～
徳安訓光	組込制御開発部	①②③④⑤⑥⑧⑨	06.12～
井上欣也	組込制御開発部	①②③④⑤⑥⑦⑧⑨⑭	06.12～
菊池達也	組込制御開発部	①②③④⑧⑨	06.12～
谷川まり子	組込制御開発部	①②③④⑤⑥⑦⑧⑨	06.12～
中村勇太	組込制御開発部	①②③④⑤⑥⑦⑧⑨	06.12～
橋本昌伸	組込制御開発部	①②③④⑤⑥⑦⑧⑨	06.12～08.11
後藤孝一	組込制御開発部	①②③④⑤⑥⑦⑧⑨	06.12～
杉山　歩	組込制御開発部	①②③④⑧⑨	06.12～07.3 08.12～09.04
渡辺友裕	組込制御開発部	①②③④⑤⑥⑦⑧⑨	06.12～
杉本明加	組込制御開発部	①②③④⑧⑨⑪⑬	06.12～07.3
熊田雄也	組込制御開発部	①②③④⑧⑨	06.12～
竹内　舞	組込制御開発部	①②③④⑧⑨	06.12～
安田尚広	組込制御開発部	①②③④⑧⑨	06.12～08.11
久保綾子	組込制御開発部	①②③④⑧⑨	07.08～09.3
山本光紗	組込制御開発部	①②③④⑧⑨	06.12～
幸　嘉夫	組込制御開発部　次長	①②③④⑧⑨	06.12～
松岡裕介	組込制御開発部　副主査	①②③④⑧⑨	06.12～
吉田健太郎	組込制御開発部　研究員	①②③④⑧⑨	06.12～
田中路貴	組込制御開発部	①②③④⑧⑨⑭	08.4～
五島　章	組込制御開発部	⑭	09.04～
兼松由佳	組込制御開発部	①②③④⑧⑨	08.12～09.04
中島浩貴	組込制御開発部	①②③④⑤⑥⑦	06.12～07.11
泉　明宏	組込制御開発部	④⑤⑥⑦⑧⑨	06.12～07.11
沼田亜美	組込制御開発部	④⑤⑥⑦⑧	06.12～07.11

二宮慎吾	制御ソフトウェア開発部 課長	④⑧	06.12～07.11
伊藤俊一	IT ソリューション部　研究員	①②③④⑧	06.12～07.11
瀬尾百代	制御ソフトウェア開発部 研究員	①②③④⑧⑨	06.12～07.11
榊原将斗	組込制御開発部	①②③④⑧⑨	06.12～07.11
窪田　淳	組込制御開発部	①②③④⑧⑨	07.08～08.3
岡本　亨	組込制御開発部　課長	①②③④⑧⑨⑪⑬	06.12～08.3
戸澤　充	組込制御開発部	①②③④⑧⑨	09.04～
石川雄大	組込制御開発部	①②③④⑧⑨⑪⑬	09.04～

【再委託先】※研究員のみ

株式会社サニー技研

〒６６４-０８５８　兵庫県伊丹市西台３-１-９

氏　名	所属・役職		実施内容	備考
中村　俊夫	MCU 応用技術部	部長	①⑭	
熊本　一信	〃	課長	①⑭	
田代　有宏	〃	課長代理	⑤⑦	
尾仲　洋和	〃	専任	①⑤⑦⑭	
作道　直樹	〃	主任	⑤⑦⑭	
田中　俊行	〃	主任	⑤⑦	
村上　倫	〃	主任	⑤⑦	
渡辺　雅之	〃	主任	⑤⑦	
清水　直人	〃		⑤⑦	
御堂　将太	〃		⑤⑦	
田中　良憲	〃		⑤⑦	
山田　真吾	〃		⑤⑦	
水野　貴文	〃		⑤⑦	
濱野　亮輔	〃		⑤⑦	
平田　勧	〃		⑤	
森下　正博	〃		⑤⑦	～'08.1
米田　真之	〃		⑤⑦	08.2～'08.5
石本　裕介	〃		⑤⑦	08.2～
中本　加那	〃		⑤⑦	08.2～

浜崎　正夫	ネットワーク技術部　　課長	①⑤⑦⑭	08.2～
西田　元彦	〃　　課長代理	①⑤⑦⑭	08.6～
田村　泰朗	〃　　専任	①⑤⑦	08.12～
多良　圭一郎	〃　　主任	⑤⑦	08.12～
森　禎道	〃　　主任	⑤⑦	08.12～
高島　光	MCU 応用技術部	⑤⑦	08.12～
中野　勇気	ネットワーク技術部	⑤⑦	08.12～09.2
今村　聡彦	MCU 応用技術部　　課長	①⑭	08.12～

東海ソフト株式会社

〒４５１－００４３　愛知県名古屋市西区新道 2 丁目 15 番 1 号

氏　名	所属・役職	実施内容	備考
安田正博	品質保証部次長	①③⑥⑦⑧⑭	
伊藤道朗	品質保証部品質保証課主査	①③⑭	
森　　聡	品質保証部品質保証課係長	①③⑭	
河合雄治	品質保証部生産技術課係長	①③⑥⑦⑧⑭	～08.5
伊藤久司	本社営業部ソリューション営業課担当課長	①③⑭	
加藤　実	エンベデッド開発部システム１課係長	⑥⑦⑧	～08.11
尾上雅憲	第３技術部システム１課係長	⑥⑦⑧	
古田　勉	エンベデッド開発部システム１課係長	⑥⑦⑧	～08.11
岡村真吾	三重支店ソリューションシステム課係長	①③⑥⑦⑧	
古田英美	三重支店ソリューションシステム課	⑥⑦⑧	
冬賀　智	第３技術部システム２課係長	⑥⑦⑧	
安江正光	第３技術部システム２課係長	①③⑭	～08.5
浅岡清徳	第３技術部システム２課主任	⑥⑦⑧	
安藤美帆	第３技術部システム２課	⑥⑦⑧	
高岸洸貴	第３技術部システム２課	⑥⑦⑧	～08.11
宮地良明	第３技術部システム１課	⑥⑦⑧	
今村友紀	三重支店ソリューションシステム課	⑥⑦⑧	
丁　長青	第３技術部システム２課	⑥⑦⑧	～08.11
野田寿希	三重支店ソリューションシステム課	⑥⑦⑧	

国立大学法人　名古屋大学

〒464-8601　名古屋市千種区不老町

氏　名	所属・役職	実施内容	備考
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・センター長	① ② ③ ④ ⑤ ⑥⑦⑧⑨⑪	
手嶋　茂晴	大学院情報科学研究科附属組込みシステム研究システム 特任教授・ディレクタ	①②③④	
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システム　助手	①②③④	

独立行政法人産業技術総合研究所

〒１００－８９２１　東京都千代田区霞が関一丁目３番１号

氏　名	所属・役職	実施内容	備考
木下　佳樹	システム検証研究センター･研究センター長	③⑪⑭	
水口　大知	計測標準研究部門計量標準システム科／システム検証研究センター・研究員	③⑪⑭	
松岡　聡	計測標準研究部門計量標準システム科／システム検証研究センター・研究員	③⑪⑭	
長谷部　浩二	システム検証研究センター・特別研究員	③⑪⑭	～08.02
前田　恒明	計測標準研究部門計量標準システム科･科長	③⑪⑭	08.12～

名古屋市工業研究所

〒４５６－００５８　名古屋市熱田区六番三丁目４番４１号

氏　名	所属・役職	実施内容	備考
月東　充	電子情報部情報・デバイス研究室　室長	⑩⑬	07.4～
小川　清	電子情報部情報・デバイス研究室	⑩⑫⑬⑭	
斉藤直希	電子情報部情報・デバイス研究室	⑩⑫⑬	
渡部謹二	電子情報部情報・デバイス研究室	⑩⑬	

北海道立工業試験場

〒０６０－０８１９　北海道札幌市北区北１９条西１１丁目

氏　名	所属・役職	実施内容	備考
堀　武司	情報システム部情報通信科　研究職員	⑩	
奥田　篤	企画調整部企画調整課　研究企画係長	⑩	
波　通隆	情報システム部　主任研究員	⑩	

(3)　委員会等

【アドバイザ】

氏　名	所属・役職	備考
川名 茂之	トヨタ自動車株式会社　制御システム統括部 制御プロセス企画室　グループ長	06.12～
城戸 正利	トヨタ自動車株式会社　制御ソフトウェア開発部 基本ソフトウェア開発室 共通ソフト PF グループ長	06.12～
細谷 伊知郎	トヨタ自動車株式会社　制御ソフトウェア開発部主査兼制御システム開発部主査	06.12～
鈴村 延保	アイシン精機株式会社　第 1 電子系技術部　主査	06.12～
草深 宗夫	アイシン・エィ・ダブリュ株式会社　技術本部 電子技術部　副部長	06.12～
稲垣 修	株式会社東海理化　エレクトロニクス技術部 プラットホーム開発室　PF 1 グループ長	06.12～
浅野 真弘	株式会社ルネサステクノロジ マイコン統括本部 主主管技師長	06.12～
香野 孝通	株式会社豊通エレクトロニクス マーケティング部　ソフトウェアイインテグレーションググループ　グループリーダー	06.12～
長谷部　浩二	筑波大学大学院　システム情報工学研究科 研究員	08.4～

【研究開発委員会日程】

＜平成 18 年度＞

開催名	開催日	開催時間	場所
第1回研究開発委員会兼第1回技術検討委員会	1月12日	15:30～17:30	㈱豊通エレクトロニクス13F会議室
第2回研究開発委員会	3月9日	13:30～15:00	安保ホール　601号室
第3回研究開発委員会	5月8日	13:30～15:30	AP名古屋．名駅　Bルーム
第4回研究開発委員会	7月4日	16:00～18:00	㈱ルネサステクノロジ那珂工場　N-3棟　講堂A
第5回研究開発委員会	8月22日	15:30～17:00	㈱アイシン精機　豊頃第1宿舎
第6回研究開発委員会	8月23日	16:30～18:30	㈱アイシン精機　豊頃第1宿舎
第7回研究開発委員会	10月9日	13:30～15:30	名古屋大学　3F会議室

＜平成 19 年度＞

開催名	開催日	開催時間	場所
第1回研究開発委員会	平成19年12月5日	13:30～15:00	AP名古屋.名駅
第2回研究開発委員会	平成20年2月12日	13:30～15:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第3回研究開発委員会	平成20年4月17日	16:30～17:30	株式会社ルネサス九州セミコンダクタ
第4回研究開発委員会	平成20年4月18日	15:30～16:00	アスコットホテル
第5回研究開発委員会	平成20年6月17日	13:30～15:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第6回研究開発委員会	平成20年8月22日	13:00～15:00	産業技術総合研究所　関西センター千里オフィス
臨時研究開発委員会	平成20年8月28日	13:00～13:10	全トヨタ労連研修センター「つどいの丘」
第7回研究開発委員会	平成20年10月14日	13:30～14:45	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室

＜平成 20 年度＞

開催名	開催日	開催時間	場所
第1回研究開発委員会	平成20年12月24日	13:30～15:00	DAITEC SAKAE 7F会議室
第2回研究開発委員会	平成21年2月13日	13:30～14:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第3回研究開発委員会	平成21年4月17日	13:30～15:00	株式会社ルネサステクノロジ　大阪半導体応用技術センター
第4回研究開発委員会	平成21年6月11日	15:30～16:00	独立行政法人産業技術総合研究所 つくば中央2-1D棟第1AV室
第5回研究開発委員会	平成21年6月12日	10:00～12:00	つくば国際会議場　小会議室304
第6回研究開発委員会	平成21年8月18日	13:30～15:00	名古屋大学　情報基盤センター4F演習室
第7回研究開発委員会	平成21年10月6日	13:30～14:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室

【技術検討委員会】

＜平成 18 年度＞

開催名	開催日	開催時間	場所
第1回研究開発委員会兼第1回技術検討委員会	1月12日	15:30～17:30	㈱豊通エレクトロニクス13F会議室
第2回技術検討委員会	1月31日	13:30～17:00	名古屋大学　3F会議室
第3回技術検討委員会	3月9日	15:00～18:00	安保ホール　601号室
第4回技術検討委員会(第1回コンサル)	4月3日	10:00～17:00	東海物産㈱　6F B会議室
第5回技術検討委員会(第2回コンサル)	4月16日	10:00～17:00	名古屋大学　3F会議室
第6回技術検討委員会	4月20日	15:00～18:00	㈱ルネサステクノロジ　7F第2･第3会議室
第7回技術検討委員会(第3回コンサル)	5月7日	10:00～16:30	名古屋大学　3F会議室
第8回技術検討委員会	5月8日	15:00～17:30	AP名古屋. 名駅　Bルーム
第9回技術検討委員会(第4回コンサル)	5月14日	10:00～16:30	名古屋大学　3F会議室
第10回技術検討委員会	6月1日	14:00～21:00	マナハウス7F
第11回技術検討委員会(第5回コンサル)	6月5日	13:30～17:00	名古屋大学　3F会議室
第12回技術検討委員会	6月11日	10:00～16:30	名古屋大学　3F会議室
第13回技術検討委員会	6月12日	10:00～21:30	㈱ルネサステクノロジ　7F第2･第3会議室
第14回技術検討委員会(第6回コンサル)	6月19日	10:00～17:00	名古屋大学　3F会議室
第15回技術検討委員会	7月4日	21:00～24:00	グランドホテル武田　会議室
第16回技術検討委員会	7月5日	9:00～12:00	グランドホテル武田　会議室
第17回技術検討委員会(第7回コンサル)	7月19日	10:00～16:00	名古屋大学　3F会議室
第18回技術検討委員会(第8回コンサル)	8月7日	10:00～16:00	名古屋大学　3F会議室
第19回技術検討委員会	8月22日	17:15～19:30	㈱アイシン精機　豊頃宿舎
第20回技術検討委員会	8月23日	20:00～22:00	㈱アイシン精機　豊頃宿舎
第21回技術検討委員会	8月24日	13:00～16:00	㈱アイシン精機　豊頃宿舎
第22回技術検討委員会	9月11日	13:30～17:00	名古屋大学　3F会議室
第23回技術検討委員会(第9回コンサル)	9月21日	10:00～16:30	東海物産㈱　6F　B会議室
第24回技術検討委員会	10月9日	15:30～17:00	名古屋大学　3F会議室
第25回技術検討委員会	10月30日	13:30～16:30	名古屋大学　3F会議室

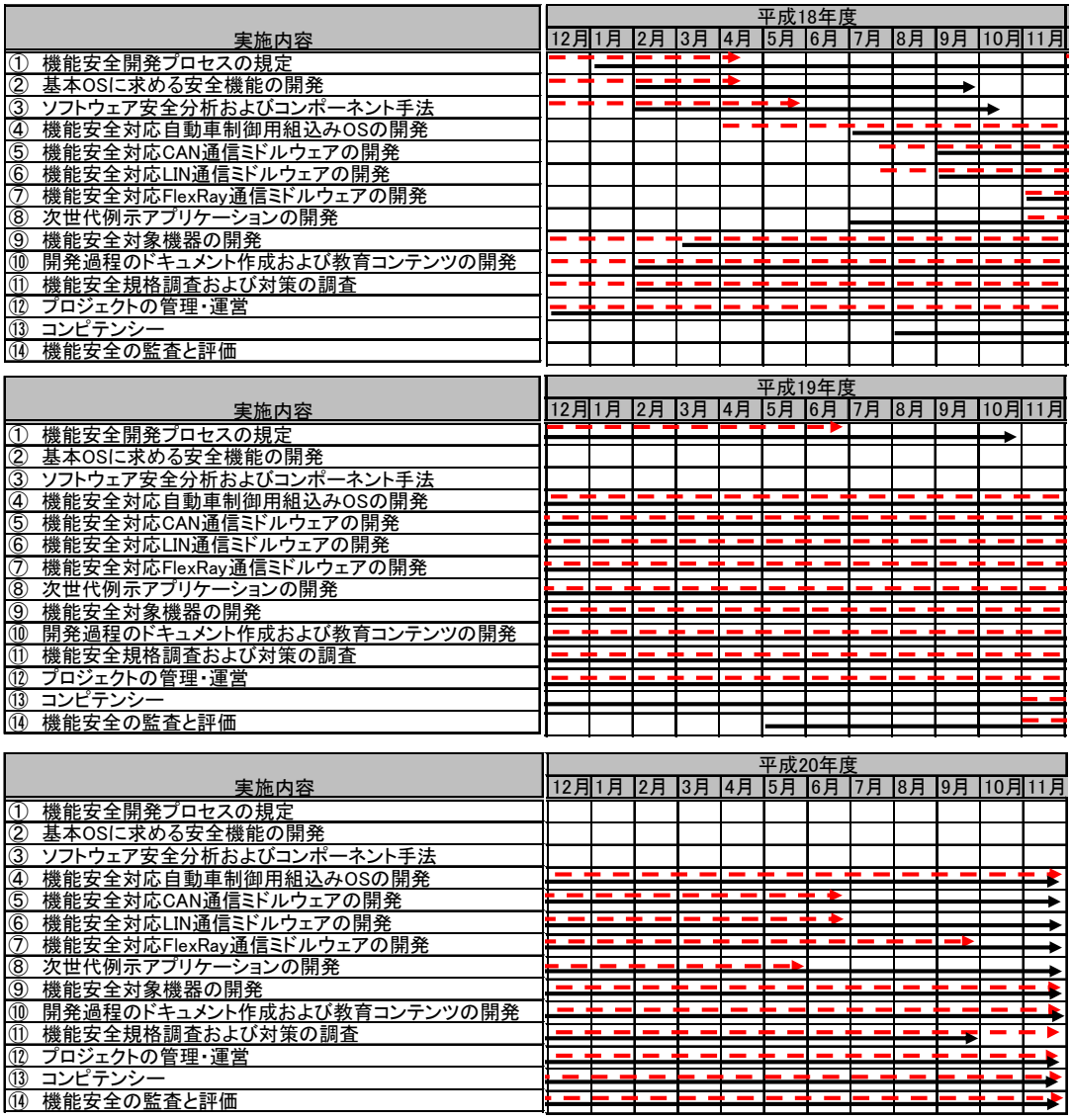
＜平成 19 年度＞

開催名	開催日	開催時間	場所
第1回技術検討委員会	平成19年12月5日	15:30～17:00	AP名古屋.名駅
第2回技術検討委員会	平成20年1月17日	13:30～17:15	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第3回技術検討委員会	平成20年2月12日	15:00～17:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第4回技術検討委員会	平成20年3月11日	13:30～15:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第5回技術検討委員会	平成20年5月20日	10:30～12:00 13:00～17:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第6回技術検討委員会	平成20年6月17日	15:00～17:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第7回技術検討委員会	平成20年7月15日	13:30～17:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第8回技術検討委員会	平成20年8月22日	15:00～17:00	産業技術総合研究所　関西センター千里オフィス
臨時技術検討委員会1	平成20年8月29日	16:20～16:50	全トヨタ労連研修センター「つどいの丘」
臨時技術検討委員会2	平成20年8月29日	16:50～17:00	全トヨタ労連研修センター「つどいの丘」
第9回技術検討委員会	平成20年9月24日	13:30～17:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第10回技術検討委員会	平成20年10月14日	14:45～17:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室

＜平成 20 年度＞

開催名	開催日	開催時間	場所
第1回技術検討委員会	平成20年12月24日	15:00～17:00	DAITEC SAKAE 7C会議室
第2回技術検討委員会	平成21年1月22日	13:30～16:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第3回技術検討委員会	平成21年2月13日	14:30～17:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第4回技術検討委員会	平成21年3月19日	13:30～16:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第5回技術検討委員会	平成21年4月17日	15:00～17:00	ルネサステクノロジ 大阪半導体応用技術センター　会議室
第6回技術検討委員会	平成21年5月19日	13:30～14:30	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第7回技術検討委員会	平成21年6月11日	16:00～17:15	独立行政法人産業技術総合研究所つくば中央2-1 D棟第1AV室
第8回技術検討委員会	平成21年6月12日	13:00～15:00	つくば国際会議場　小会議室304
第9回技術検討委員会	平成21年7月14日	13:30～15:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第10回技術検討委員会	平成21年8月18日	15:00～17:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第11回技術検討委員会	平成21年9月15日	13:30～17:00	名古屋大学　東山キャンパス　IB電子情報館南東3階　会議室
第12回技術検討委員会	平成21年10月6日	14:30～17:00	名古屋大学　東山キャンパス　IB電子情報館南東5階　会議室

(4)　スケジュール



補足：破線赤字矢印は計画を示し、実線黒字矢印は実績を示す

３．成果概要

本研究の大きな目標として①機能安全に対応した自動車制御用組込み OS の開発 ②機能安全に対応した自動車通信ミドルウェアの開発と次世代車両例示アプリケーションの開発 であり、この副次目標として ③機能安全対策予備実験 ④開発成果物の模擬認証 ⑤第三者が再現可能な機能安全模擬認証対象機器の開発 である。以下にその概要を記す。

① 機能安全に対応した自動車制御 OS の開発は完了した。この OS は当初“保護機能”を有する OS を計画していたが、機能安全対応をするに当り、保護機能は必須でなく、その OS の故障を検出する機能が必須でることが欧州調査等により判明した。そのため、研究途中に保護機能開発を中止し、“故障検出ライブラリ”の開発を行ない、機能安全対応 OS として完成させた。

② 機能安全に対応した CAN 通信ドライバ及び FlexRay 通信ドライバの開発完了と LIN 通信モジュールの開発を完了させた。

③ IEC 61508 SIL (Safety Integrity Level) 3 取得に必要な項目（安全分析・開発手法）を実験的に実施し、その実施ノウハウを蓄積することである。本研究では、基本安全分析手法 3 種と独自のソフトウェアコンポーネント分析を考案し、実験的に適応した。また、規格が要求する開発手法も全て実験的に適応し、かつ、SIL3 以上で求められているフォーマルメソッド 3 種につても実験適応した。これらの成果物として各種手法マニュアルを作成している。

④ 開発ソフトウェアは機能安全規格に準拠した開発を行ない、妥当性検証、監査及び評価を実施し、第三者機関による模擬認証を行なうことである。

本研究では第三者機関として独立法人産業総合研究所 システム検証研究センター 職員が模擬的な認証機関となり、開発ソフトウェアの認証を実施した。尚、認証等の内容については、国際認定機関である TUV_SUD と技術的なディスカッションを行い、その妥当性を確認している。

模擬認証としての結果は、概ね国際認証機関で認証取得が可能なレベルであると報告を受けている。

⑤ 本研究関係外の機関が機能安全認証を取得するために、本研究成果を利用し、模擬的に再現することが可能な機器を開発することである。すなわち、本研究内で利用した対象機器（電動カート）の開発となる。

本研究では、電動カートの構成機能のうち、ブレーキ機能について機器開発を実施した。この開発機器の利用条件は特に設ける予定でないため、本研究関係外の機関が本研究開発成果（ソフトウェア、各種ドキュメント）と開発機器を利用して再現可能な成果が得られる。

補足）本研究の開発成果（ソフトウェア、各種ドキュメント）と開発機器資料はオー

プンソースとして一般公開を予定している。

上記報告の通り、本研究当初に計画した開発成果は、若干の修正があるものの全て目標に達成したレベルで完了したことを報告する。

４．当該研究開発の連絡窓口

株式会社 ヴィッツ
〒４６０－０００８ 愛知県名古屋市中区栄二丁目１３番地１号　白川第２ビル
ＴＥＬ:０５２-２２０-１２１８　　ＦＡＸ:０５２-２１８-５８５５
担当者 ： 会長　　安場　尚一
総務部　　佐藤　倫子

第２章　本論

１．機能安全対応自動車制御用組込み 0S

機能安全対応自動車制御用組込み OS（以下 Safe OS と記載）の開発について、機能安全対応にて求められる内容を中心に記載する。

①　安全コンセプト（Safety Concept ）

Safe OS の安全コンセプトについて記載する。なお、本研究ではソフトウェアの機能安全対応に広く参考となるよう、ハードウェアの違いを意識しなくて良い部分に焦点を当てている。安全コンセプトの概要を以下に記載する。

ⅰ　自動車制御システムを中心に、広く組込み制御システムで利用可能な OS とす。

ⅱ　以下２つの構成で、各安全目標を満たす OS とする。

1)　故障検出機能を有し、フォールトトレランス性のあるハードウェアでは、安全目標を SIL3 とする。

2)　上記を満たさないハードウェアでは、安全目標を SIL2 とする。

ⅲ　uITRON 仕様 OS の機能の内、故障要因をはらむ機能や、安全関連系のシステムで必須ではない機能を削除する。

ⅳ　システム全体で故障検出をするために利用可能な、故障検出機能をライブラリとして提供する（故障検出 90%～99%を実現可能な機能)。

ⅴ　サブセット化した OS 機能（以下カーネルと記載）と、故障検出ライブラリを合わせて、Safe OS とする。

ⅵ　規格より、安全目標 SIL3 で必須の手法（プロセス）にて Safe OS を開発する。

ⅶ　Safe OS を安全に利用するための、安全機能開発ガイドラインを作成する

上記コンセプトを検討、決定するにあたり、以下の分析を行った。

ⅰ　OS の API に着目し、API を実行してもその効果が得られない原因について分析した。分析手法としては FTA を用い、故障モードを想定するために HAZOP で用いるガイドワードを利用した。

ⅱ　分析結果より必要な対策を、故障検出ライブラリとして用意した。

ⅲ　Safe OS 全体として、再度分析を行い、全ての故障モードに対して、漏れかつ矛盾のない対策が用意できていることを確認した。

上記コンセプトおよび分析結果より、Safe OS を下図のような構造とした。

また、Safe OS 全体での分析概要および、故障モードへの対策概要を、下表に示す。なお、検討が必要な項目が１箇所あるが、これについては設計時に行うモジュールレベルでの分析にて、対策の検討を行う。

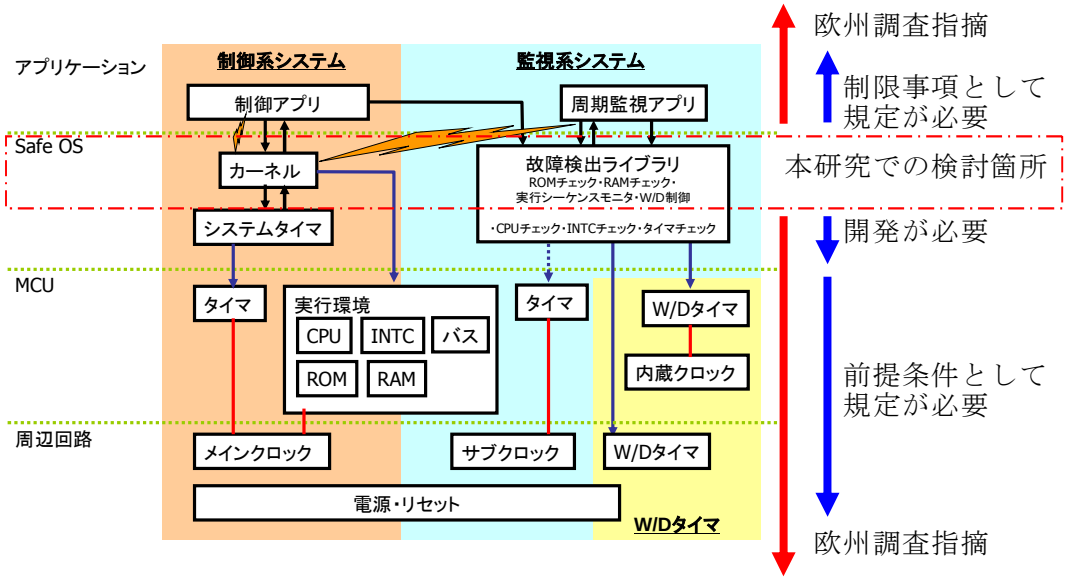


図 1　Safe OS 全体像

表 1　Safe OS 故障対策

故障モード	影響	対策	
制御処理順序がおかしい	監視処理への通知がおかしい	通知順序を監視	制御系システムの故障は監視系システムで検出する。
制御処理未実行	監視処理への通知がない	デッドライン時刻を監視	
制御処理周期が早い	監視処理への通知が早い	開始時刻を監視	
制御処理周期が遅い	監視処理への通知が遅い	デッドライン時刻を監視	
監視処理で異常未検知	異常のまま動作を継続する	検討が必要	監視系システムの故障は自己検出、または、W/D にてリセットする。
監視処理未実行	W/D未キャンセル	不要 (リセットにより安全側に動作)	
監視処理周期が早い	W/Dキャンセルが早い	連続キャンセル禁止時間を監視	
監視処理周期が遅い	W/Dキャンセルが遅い	不要 (リセットにより安全側に動作)	
W/Dタイマがリセット信号を出さない	安全側に動作しない	システム起動毎にW/Dタイマの故障診断を行う	W/D タイマの故障は制御系システムで検出する。

最終年度の欧州調査において、以下の指摘を受けており、対策が必要である。

i　機能安全対応をするには、Safe OS にハードウェアに依存する部分を含める必要がある。なお、全体像は上記の構成で良いと考えている。

ii　故障検出ライブラリについては、対応するハードウェアを特定し、ハードウェアアーキテクチャに合わせた要求仕様とする必要がある。

iii　安全機能ガイドラインには、アプリケーションへの制限事項だけでなく、どのように使用すると、Safe OS を安全に利用できるかを記載する必要がある。

iv　ソフトウェア安全要求仕様書には、性能に関する要求も記載する必要がある。

② 機能安全開発管理規定（Functional Safety Management Plan ）

機能安全開発に必要な FSMP には、下表（FSMP 項目一覧）に示す内容の記載が必要である。

表 2　FSMP 項目一覧

項目	概要
安全目標	本開発で目指す SIL。
システムの対象範囲	本開発における機能安全対応の対象とするシステムの範囲
組織情報	組織図、各部署の役割・責任、作業担当者情報
スキル情報	作業担当者の能力、能力の判断方法
リスク管理	想定されるリスクに対する対処方法
コミュニケーション方法	組織内外におけるコミュニケーション方法
ドキュメント体系	ドキュメント一覧、ドキュメント ID の定義、ドキュメント構成図
構成管理方法	構成管理の手順、構成管理に使用するツールの信頼性
トレーサビリティ管理方法	トレーサビリティ管理の手順、トレーサビリティ管理に使用するツールの信頼性
機能安全評価方法	機能安全評価の手順、判断基準、担当者
開発工程の定義	各開発工程について、作業手順と成果物の定義
適合確認方法	適合確認の手順、判断基準、担当者

トレーサビリティ管理方法、安全目標及びシステムの対象範囲を明確にすることが、機能安全開発の特徴である。なお、安全目標とシステムの対象範囲はコンセプトで示す内容と一致している必要がある。トレーサビリティ管理は、要求・設計・テストの関連する項目を追跡調査するための以下の情報を管理する。

i　各開発工程における成果物の妥当性証明

ii　ソフトウェア変更時の影響分析

本研究におけるトレーサビリティ管理として、以下を実施した。

i　成果文書内の要求・設計・テスト項目毎にユニークなトレーサビリティ番号を記載する。

ii　上記項目を記載する根拠となった参照元のトレーサビリティ番号を記載する。

iii　トレーサビリティ番号間の関連を、要求管理ツール RaQuest で管理する。

③　開発ソフトウェアおよび設計ドキュメント

Safe OS のソフトウェア構成を、下図に示す。

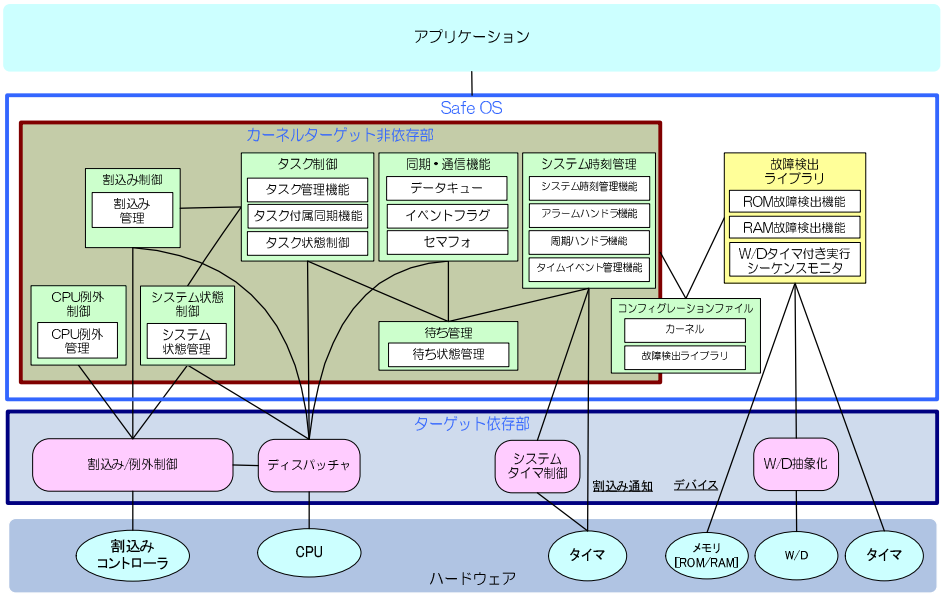


図 2　Safe OS のソフトウェア構成

カーネルの機能は前述のコンセプトのとおり、uITRON 仕様のサブセットであり、開発した全ての機能は互換性を持っている。

故障検出ライブラリは、ハードウェア依存しない、以下機能を開発した。

ⅰ　電源投入時、処理動作時両方のタイミングで故障検出が行える、メモリ（ROM/RAM）故障検出機能。

ⅱ　制御処理からの通知をモニタすることで、処理の順序および、開始・終了時刻を監視する機能と、W/D のキャンセル時刻を監視する機能を併せ持った、W/D タイマ付実行シーケンスモニタ。

上記 Safe OS の開発において作成した設計書を、下表に記載する。

表 3　設計ドキュメント一覧

ドキュメント名称	概要
ソフトウェアアーキテクチャ設計書	機能（モジュール）分割設計
	オブジェクトおよび管理データ設計
	モジュール間の I/F 設計
	処理シーケンス設計
	トレーサビリティ番号付けおよび管理
ソフトウェアシステムテスト計画書	テスト環境およびテスト実施方法
	テスト項目
	トレーサビリティ番号付けおよび管理

ソフトウェアモジュール設計書	ディレクトリおよびファイル構成	
	モジュール詳細設計	関数
		モジュール内データ
		データ型
		マクロ
		詳細フロー
	トレーサビリティ番号付けおよび管理	
ソフトウェアモジュールテスト計画書	テスト環境およびテスト実施方法	
	テスト項目	
	トレーサビリティ番号付けおよび管理	

設計書の作成は FSMP に記載された手順に従っており、機能安全対応の特徴の一つであるトレーサビリティ番号の管理が、全てのドキュメントで対応されている。

最終年度の欧州調査において、以下の指摘を受けており、対策が必要である。
データに対する設計がされていない。また、データ設計に基づいたテスト設計がされていない。

④　適合確認と監査

適合確認は、入力情報と成果物を比較し、成果物に問題が無いことを、第 3 者の観点から確認することである。適合確認は開発工程ごとに実施する。

監査は、FSMP に記載されたとおりの開発プロセスが実施されているかを確認することである。本研究では、以下を考慮し、適合確認と一緒に実施した。

ⅰ　精度が高い。
ⅱ　確認作業の効率が高い。
ⅲ　修正による差し戻しへの対応が可能。

本研究における適合確認のチェック項目を、ソフトウェアアーキテクチャ設計工程を例に、以下に記載する。他の開発工程についても同様のチェック項目を用意している。

表 4　適合確認チェック項目

大項目	中項目	小項目	概要
ソフトウェアアーキテクチャ設計書	設計項目	トレーサビリティ	規格に記載されている適合確認への要求事項について確認する。
		安全性	
		試験性	

		一貫性	
		読解性	
		修正性	
	データ項目	許容範囲	
		データ構造	
		データ異常への対策	
		データ破壊への対策	
ソフトウェアシステムテスト計画書	テスト項目	トレーサビリティ	
		テスト環境・テスト手順	
適用手法の評価	ソフトウェアアーキテクチャ設計		規格で要求されている手法の適用有無を確認する。
	ソフトウェアシステムテスト		
使用ツールの信頼性評価	ソフトウェアアーキテクチャ設計		開発に使用した全てのツールについて、信頼性を評価する。
	ソフトウェアシステムテスト		
監査	ソフトウェアアーキテクチャ設計		FSMP に記載された作業項目通りに作業が実施されているかを確認する。
	ソフトウェアシステムテスト		

全チェック項目について、以下 3 段階の基準にて良否判定を行った。

ⅰ　合格：チェック項目を満たしていると判断できるもの。

ⅱ　条件付合格：チェック項目を満たせていないが、次工程への影響が小さいもの。

ⅲ　不合格：チェック項目を満たせておらず、次項目への影響が大きいもの。

Safe OS の開発における適合確認も、上記チェック項目および良否判定基準にて行った。チェック項目や良否判定基準について過不足は見受けられなかった。

⑤　開発の総括

安全コンセプトに従い、ソフトウェア安全要求仕様書に規定された Safe OS を、FSMP に規定された開発プロセスに沿って開発した。開発は完了したが、前記のとおりハードウェアに依存する部分の開発も必要である。

ハードウェア依存部を含む機能安全対応自動車制御用組込み OS を完成させるには、

もうしばらくの時間が必要である。なお、本研究で実施したプロセスでハードウェアに依存する部分を開発することで、機能安全対応自動車制御用組込み OS を完成させることが可能である。

２．機能安全対応 CAN 通信ミドルウェア

①　安全コンセプト（Safety Concept ）

機能安全対応 CAN 通信ミドルウェアは、安全機能を搭載した CAN 通信ミドルウェア ドライバ(以下 DRV と省略)モジュールについて開発した。

安全コンセプトとしては、通信における故障検出の機能および、H/W の故障検出機能を実装した CAN 通信ミドルウェアのドライバモジュールを IEC61508-3 に規定される SIL 3(Safety Integrity Level;安全要求度水準) の HR (High Recommend) 手法で開発した。

また、CAN 通信の安全分析を実施する上で、IEC61784-3-2 の「通信エラーと検出方法マトリクス」を元に、独自の通信エラー分析を行い、CAN プロトコルを含めた分析を実施した。

本通信ミドルウェアを使用して、機能安全対応システムを開発する際には、そのシステムに対する安全分析を行った上で、上位アプリケーションに安全機能が必要かどうかを判断し実装していただく必要がある。

②　機能安全開発管理規定（Functional Safety Management Plan ）

「機能安全対応自動車制御用組込み OS」にて規定された管理規定を CAN 通信開発に適用した。適用に際し、特記するべき差異はない。

③　開発ソフトウェアおよび設計ドキュメント

＜開発ソフトウェア＞

CAN 通信ミドルウェアに安全分析を組み込んだソフトウェアを開発する。

開発範囲は、通信ミドルウェアの中のドライバのみとする。

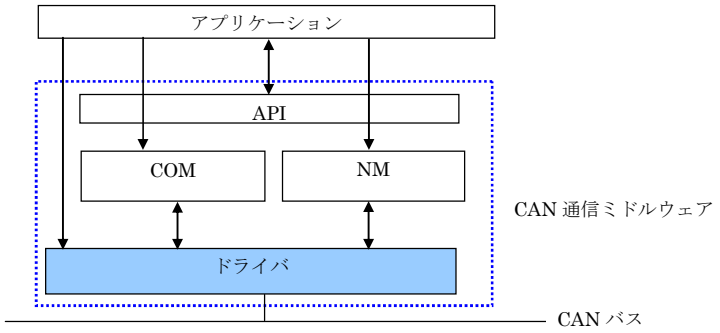


図 3　CAN 通信ミドルウェアの構成図

CAN 通信ミドルウェアのドライバに実装する機能を以下に記述する。

表 5　CAN 通信ミドルウェアの機能一覧表

機能名	概要
送信制御機能	フレームの送信を行う。
受信制御機能	フレームの受信を行う。
バスオフ検出機能	バスオフの検出状態をアプリケーションへ通知を行う。
CAN コントローラ制御	CAN コントローラの制御を行う。
レジスタライト/リード機能	特定のレジスタに対して書き込みを実施し、読み込んだ値が同等となることをチェックする。
レジスタ化けチェック機能	動作中は書き換わらない箇所に対して、設定値が正しいかのチェックを行う。

＜設計ドキュメント＞

CAN 開発で作成する設計ドキュメントを以下に記す。

表 6　CAN 開発の設計ドキュメント一覧

ドキュメント名称	概要
CAN 通信ミドルウェア機能安全対応開発計画書	機能安全対応 CAN 通信ミドルウェアの開発プロジェクトの実施計画書に該当
車載用 CAN 通信ミドルウェア仕様書	CAN 通信ミドルウェアの機能仕様書
E/E/PES 安全要求仕様書	安全分析結果から安全機能について記述した仕様書
ソフトウェア安全要求仕様書	ソフトウェア要求仕様工程で作成する。 車載用 CAN 通信ミドルウェア仕様書と E/E/PES 安全要求仕様書から、CAN 通信ミドルウェアの安全に関する要求仕様書
ソフトウェアアーキテクチャ設計書	CAN 通信ミドルウェアのソフトウェアの構成について記述する基本設計書
コーディング規約書	コーディング規約について記述する規約書
ソフトウェアモジュール設計書	CAN 通信ミドルウェアのモジュール単位について記述する詳細設計書
ソースコードリスト	ソースコードのリスト
ソースコードレビュー報告書	ソースコードのレビュー結果の報告書

コーディングルール逸脱手続書	コーディングルールを逸脱した際に逸脱理由を記述
ソフトウェアモジュールテスト計画書兼報告書	モジュールテスト計画書兼テスト結果の報告書
ソフトウェアシステムテスト計画書兼報告書	システムテスト計画書兼テスト結果の報告書

④　適合確認と監査

適合確認項目と判定基準の概要について以下に記載する。

表 7　適合確認項目表

確認項目	内容	判定基準
安全性	安全機能が正しく動作すること。	目的とする安全度に応じた手法を使用しての設計ができていること。 安全機能が正しく動作すること。
試験性	安全機能が正しく試験できること。	試験に関する手法が適用できる記載があること。
トレーサビリティ	文書間の要求に過不足がないこと。	要求管理ツールにより、要求のトレーサビリティがとれていること。
一貫性	文書間の記述に食い違いがないこと。	文書間で関係する要求内容に食い違いがないこと。
読解性	開発者にとって不明な記述がないこと。	不明な用語がないこと、図表の表記法に十分な説明があること。

実際の判定においてはIEC61508に記載されている手法が適切に使用されているかを確認して判定する。

特にCAN通信ミドルウェアとして以下の点も確認する必要がある。

ⅰ　CAN通信によるエラー発生時に安全な処理を行えること

ⅱ　CAN通信ミドルウェアのドライバ部分については、マイコンのCAN機能が適切に使用されていること

⑤　開発の総括

既存のCAN通信プロトコルは、送信メッセージ衝突をプロトコルにて判定・再送信を実施している。しかし、バス負荷状況により、再送信不可及び再送信タイミング遅延が発生する問題があり、このままでは安全性上問題がある。そのため、CAN通信の安全機能は、次世代車載通信ネットワークとして注目されているFlexRay通信と

比較し、多くの対策を通信ミドルウェアの安全機能として対策しなければならない。

一方、CAN 通信プロトコルは ISO 11898 として国際規格化されて 10 数年経過し、これら問題の多くは、OSEK/VDX 等の標準規格団体が OSEK/VDX Communication 仕様として対策されている。ただし、これらの規格はミドルウェア部位に注力され、個別マイコンの故障モードの対策までには至っていない。

本研究では、機能安全の視点から、通信ドライバに要求される安全対策を安全機能として追加することに成功した。

CAN 通信プロトコルは、車載関連をはじめ多くの分野で広く利用されており、広範囲な分野で本通信ミドルウェアを適用した機能安全対応システムを構築することが可能となった。

3．機能安全対応 LIN 通信ミドルウェア

①　安全コンセプト（Safety Concept ）

機能安全対応 LIN 通信ミドルウェアは、安全機能を搭載した LIN 通信ミドルウェア COM モジュールについて開発した。

尚、安全コンセプトの決定および開発手法は機能安全対応 CAN 通信と同様であり、特記すべき差異はない。

②　機能安全開発管理規定（Functional Safety Management Plan ）

「機能安全対応自動車制御用組込み OS」にて規定された管理規定を LIN 通信開発に適用した。適用に際し、特記するべき差異はない。

③　開発ソフトウェアおよび設計ドキュメント

＜開発ソフトウェア＞

LIN 通信ミドルウェアに安全分析を組み込んだソフトウェアを開発する。

開発範囲は、通信ミドルウェアの中の COM モジュールのみとする。

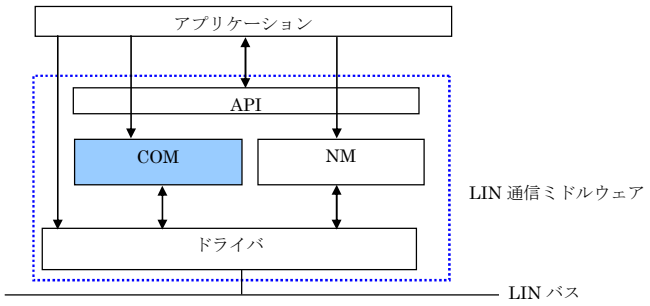


図 4　LIN 通信ミドルウェアの構成図

＜設計ドキュメント＞

LIN 開発で作成する設計ドキュメントを以下に記す。

表 8　LIN 開発の設計ドキュメント一覧

ドキュメント名称	概要
機能安全対応開発計画書	機能安全対応 LIN 通信ミドルウェアの開発プロジェクトの実施計画書に該当
ソフトウェア安全要求仕様書	機能安全対応 LIN 通信ミドルウェアへの安全要求仕様
ソフトウェア安全妥当性確認計画書	安全妥当性確認のための計画書
ソフトウェアコンポーネントアーキテクチャ設計書	LIN 通信ミドルウェアのソフトウェア構成について記述する基本設計書
ソフトウェアシステム・コンポーネントテスト計画書	LIN 通信ミドルウェアのコンポーネントレベルのテスト計画書
ソフトウェアモジュール設計書	LIN 通信ミドルウェアのモジュール単位について記述する詳細設計書
ソフトウェアモジュールテスト計画書	LIN 通信ミドルウェアのモジュールレベルのテスト計画書
機能安全ガイドライン	機能安全 LIN 通信ミドルウェアを利用するための導入ガイドライン
ソフトウェア適合確認計画書兼報告書	LIN 通信ソフトウェアの適合確認計画およびその適合確認報告書

④　適合確認と監査

機能安全対応開発計画書に従い、開発時に要求される各種手法が適切かつ正確に利用されているかを確認する。

⑤　開発の総括

本研究開発では LIN 通信ミドルウェア全てを開発するのではなく、COM モジュールに限定したが、機能安全開発の全工程を実施したことは有益であった。また、COM モジュールを開発することにより、LIN 通信はもとより CAN 通信など他の通信プロトコルへの容易な適用が可能となり、部品として価値の高い成果が得られた。

４．機能安全対応 FlexRay 通信ミドルウェア

①　安全コンセプト（Safety Concept ）

機能安全対応 FlexRay 通信ミドルウェアは、安全機能を搭載した FlexRay 通信ミドルウェア DRV モジュールについて開発した。

尚、安全コンセプトの決定および開発手法は機能安全対応 CAN 通信と同様であり、特記すべき差異はない。

② 機能安全開発管理規定（Functional Safety Management Plan ）

「機能安全対応自動車制御用組込み OS」にて規定された管理規定を FlexRay 通信開発に適用した。適用に際し、特記するべき差異はない。

③ 開発ソフトウェアおよび設計ドキュメント

＜開発ソフトウェア＞

FlexRay 通信ミドルウェアに安全分析を組み込んだソフトウェアを開発する。

開発範囲は、通信ミドルウェアの中のドライバのみとする。

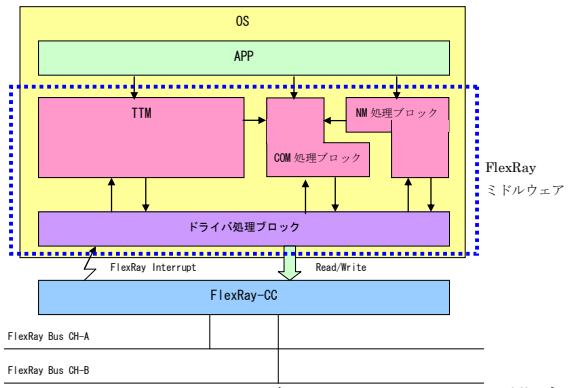


図 5 FlexRay 通信ミドルウェアの構成図

FlexRay 通信ミドルウェアのドライバに実装する機能を以下に記述する。

表 9 FlexRay 通信ミドルウェアの機能一覧表

機能名	概要
FlexRay-CC の初期化機能	DRV 初期化タイミングで FlexRay-CC の初期化を実施する。
FlexRay-CC ステート遷移機能	FlexRay-CC の状態を遷移させる。
フレーム送信機能	渡された送信データをメッセージバッファに設定する。
フレーム受信機能	メッセージバッファの受信の有無を確認して上位に渡す。
レジスタライト/リード機能	特定のレジスタに対して書き込みを実施し、読み込んだ値が同等となることをチェックする。
NM ベクタ公開機能	FlexRay-CC で管理している NM ベクタ情報を公開する。

レジスタ化けチェック	固定値のレジスタが化けていないかのチェックを実施する。
FlexRay-CC 依存機能	通信ミドルを構築する上で FlexRay-CC に依存する

＜設計ドキュメント＞

FlexRay 開発で作成する設計ドキュメントは、CAN 開発における設計ドキュメントと同種であるため、ここでは省略する。

④　適合確認と監査

適合確認項目と判定基準は、CAN 開発における適合確認項目と同一であるため、ここでは省略する。

尚、FlexRay 通信ミドルウェアとして特に確認する項目を以下に列記する。

ⅰ　FlexRay 通信によるエラー発生時に安全な処理を行えること

ⅱ　FlexRay 通信ミドルウェアのドライバ部分については、マイコンの FlexRay 機能が適切に使用されていること

ⅲ　FlexRay ドライバについては通信速度が高速になるため時間的な制約についても十分な考慮がされていること

⑤　開発の総括

FlexRay 通信プロトコルは、現世代車載通信として利用されている CAN 及び LIN と比較し、通信速度ばかりでなく、安全対策もプロトコルレベルで対策されていることが通信の安全分析により明確となった。しかし、通信プロトコルの多機能に伴い、通信 DRV モジュールの設計・開発が複雑になったことも事実である。

本研究では、FlexRay プロトコルの通信安全分析より、マイコンの故障やソフトウェアの誤使用における脅威を検出するための安全機能を追加し、更なる安全対策を施すことに成功した。

FlexRay 通信は、本研究により性能面、安全面でも他の通信より優れていることが明確になり、今後、車載を含め多くの安全機器分野での適用が求められると考える。その場合に本通信ミドルウェアが安全機器開発を支援することを期待する。

5．機能安全対応例示アプリケーション

①　安全コンセプト（Safety Concept）

例示アプリケーションは、制御対象となる電動カート上で稼動するソフトウェアを機能安全開発に準じて開発する。対象が自動車ソフトウェアであり、自動車の基本機能である“走る”“曲がる”“止まる”を実現する機能に着目するが、全ての機能を研究期間内で実現するのは不可能である。そのため、開発対象を最も安全に関係するブレーキ機能（ハードウェア構成、ソフトウェア構成を含む）と規定した。

安全コンセプトの導出方法は、レーシングカート開発の依頼者（要求者）の意見から“仮安全コンセプト”と“安全目標”を決定した後に、安全分析を実施し規定した

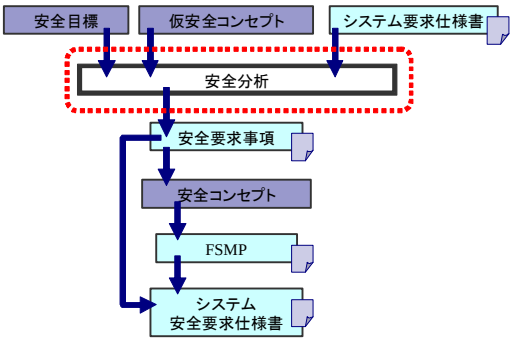


図 6　開発フローチャート

「安全分析」の目的は、安全要求事項を規定することであり、その分析条件を以下と規定した。

安全分析対象：カートシステムのブレーキ機能

分析範囲：オペレータがブレーキペダルを踏んでからタイヤが減速／停止するまでに含まれる（動作する）ハードウェア・ソフトウェア

分析方法としては、分析対象を細分化した論理ブロックを用い、HAZOP で利用されるカードワードを利用して故障事象を網羅的に抽出した。その次に、抽出した故障事象を FTA 分析により原因と対策を導出した。

② 機能安全開発管理規定（Functional Safety Management Plan）

「機能安全対応自動車制御用組込み OS」にて規定された管理規定をブレーキ機能ソフトウェア部位の開発に適用した。適用に際し、特記するべき差異はない。

ただし、ブレーキ機能開発にはハードウェア部位の開発も含めているが、本研究ではソフトウェアを対象とするため、ハードウェア部位の開発管理は対象外とした。

③ 開発ソフトウェアおよび設計ドキュメント

＜開発ソフトウェア＞

カートシステムにはステアリング制御、ブレーキ制御、アクセル制御が必要であり、以下にカートの写真とカートシステム全体のブロック図を示す。尚、機能安全開発は下記ブロックのブレーキ機能（赤枠）に限定している。

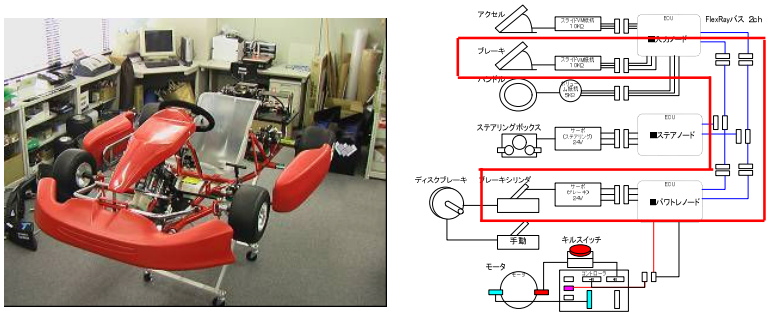


図 7　カート写真とカートシステムのブロック図

＜開発ドキュメント＞

ブレーキ機能開発で作成する設計ドキュメントを以下に記す。

表 10　ブレーキ開発の設計ドキュメント一覧

ドキュメント名称	概要
E/E/PES 安全要求仕様書	安全分析から抽出された分析結果をもとに E/E/PES 安全要求事項を規定する。
E/E/PES ハードウェア構成設計書	ハードウェア構成（基板ポートアサイン、コネクタピンアサイン、回路図、接続図）を規定する。
ソフトウェア安全要求仕様書	ソフトウェアの要求事項(安全要求事項)を IEC 61508-3 にて規定されている 10 種類の安全機能について明確化している。
ソフトウェア妥当性確認計画書	ソフトウェア安全機能の要求事項の妥当性確認計画を規定する。
ソフトウェアコンポーネント設計書	モジュールに分割とモジュールにて行うべき処理やモジュール間の関係を規定する。
ソフトウェアコンポーネントテスト計画書	コンポーネントへの要求事項を確認するためのテスト計画書を規定する。
デバイスドライバコンポーネント設計書	デバイスドライバの処理や他コンポーネント関係を規定する。
ソフトウェアモジュール設計書	モジュール化、試験可能性及び安全な修正の能力を得られるようなソフトウェアモジュールの仕様を規定する。

④　適合確認と監査

ブレーキ開発にて実施した適合確認項目を下記に記載する。

ｉ　ソフトウェア安全要求仕様工程

「ソフトウェア安全要求仕様書」及び「ソフトウェア妥当性確認計画書」への

適合確認を実施した。ソフトウェア安全要求仕様工程時の適合確認結果は「条件付受容・試験待ち」となった。

ii　ソフトウェアアーキテクチャ工程

「ソフトウェアアーキテクチャ設計書」及び「ソフトウェアシステムテスト計画書」への適合確認を実施した。ソフトウェアアーキテクチャ工程時の適合確認結果は「条件付受容・試験待ち」となった。

⑤　開発の総括

本研究でのブレーキ機能開発は、設計フェーズは完了し動作するアプリケーションは完成したものの、検証フェーズは未実施となった。ブレーキ機能開発は、単にアプリケーションソフトウェアを開発するだけでなく、ブレーキ機構のハードウェア（メカ・エレキ）を含めての開発であったため、安全分析の結果から作成する安全要求事項はハードウェア及びソフトウェア双方の仕様書を作成することとなった。これにより、ハードウェアを含めた“システム”での開発を実現し、機能安全規格が対象とする“安全システム”開発の貴重な経験を得ることができた。しかし、ハードウェアの対策は故障率を考慮した専用部品の開発が必要となり、期間および費用の関係上、規格に合致した開発はできなかったが、ハードウェア部位の機能安全規格対応方法などの調査・分析ができたことの意義は大きい。

今後、国内での機能安全対策が必要となる多くの場合、機能安全対応部品（ハードウェア・ソフトウェア）を利用し、システムを実現する事例が圧倒的に多いと考える。本ブレーキシステム開発は、このような機能安全対応部品を利用し、目指す安全度水準を得るための開発指針となると考える。

6．国際認証機関による評価について

①　国際認証機関による認証プロセスについて

機能安全の認証に際して、認証機関では IEC 61508 が規定している機能安全評価（FSA; Functional Safety Assessment）と同等の作業を実施している。機能安全評価とは、ライフサイクルの各フェーズにおける活動や成果物を詳細に検討して、規格の目的および要求事項が満たされているかどうか、そして、安全関連系によって機能安全が達成されているかどうかの判定を下す作業である。判定結果が合格であれば、国際認証機関より認証書が発行される。

国際認証機関では、IEC 61508 への適合認証を、コンセプトフェーズ、ディテールフェーズ（場合により、“実現フェーズ”と呼ぶ場合がある）、および、認証フェーズの 3 段階に分けて順次実施している。認証フェーズは、認証書を発行するだけの手続きであり、実質的な評価作業は、他の 2 つのフェーズで行われる。

② コンセプトフェーズ(Concept phase)

コンセプトフェーズにおいては、安全要求仕様の確認が行われる。そのためには、機能安全達成の方針について述べた安全コンセプトをまとめておく必要がある。加えて、アーキテクチャの安全分析（FMEA）の結果が必要になるため、コンセプトフェーズとはいえ、ある程度設計作業に入っておく必要がある。

加えて、マネジメント体制の評価が行われる。すなわち、機能安全開発管理規定（FSMP）のチェック、および、それに基づく現地監査が実施される。これには、関連する手順書や品質管理規定類の確認、開発者のコンピテンシの確認、開発に使用するツールが信用できるものであるかの確認も含まれる。

③ ディテールフェーズ（detail phase)

ディテールフェーズでは、コンセプトフェーズに続いて作成されたすべてのドキュメントのレビューが行われる（設計書、ソースコード、テスト計画書・報告書、適合確認計画書・報告書、妥当性確認計画書・報告書、安全マニュアルなど)。また、実装の終盤において、故障対策が十分であることを確認するための詳細 FMEA が必要となる。さらに最後には、故障対策が正しく実装されていることを確認するための、フォールト挿入テスト（FIT; Fault Insertion Test）が行われる。

④ 国際認証機関への調査で明確になった認証に必要な事項

認証取得で特に重要と思われる点を、国際認証機関からの指摘事項に基づいて、以下にまとめる。

ⅰ 製品の安全コンセプトを明確に文書化しなければならない。安全コンセプトの中身自体は商品価値に関する部分なので、その是非が問題になる可能性は低いと思われる。しかしながら、どのように機能安全を目指すのかという方針を認証機関に明確に伝えて完全に理解してもらうことが、その後の認証を円滑に進めるためには重要となる。

ⅱ 安全関連部分と非安全関連部分の境界を明確に示さなければならない。安全関連部分においては、安全維持のための機能（SIF; Safety Integrity Function）として、どのような機能を備えているかを明確にしなければならない。

ⅲ ソフトウェアが動作の前提とするハードウェア環境を明確に示さなければならない。それが認証の条件となるためである。

ⅳ ソフトウェアのみの製品であっても IEC 61508-3 だけでなく、IEC 61508-2 を参照する必要がある。故障診断率とハードウェアアーキテクチャによって安全度水準の上限が規定されており、故障診断機能はソフトウェアによって実現されることもあるためである。特に、IEC 61508-2 に記載されているハードウェアの故障モードのリストをどのようにカバーするかについて明確にしなければなら

ない。

v　安全分析を FMEA によって完全に実施し、すべての故障モードを網羅しなければならない。分析結果を踏まえて、十分な故障対策がなければならない。故障対策を利用者に委ねる場合には、そのことを安全マニュアルに明記しなければならない。

vi　開発に先立って、機能安全開発管理規定（FSMP）を明確に定めなければならない。その際、規格が実施を要求している開発フェーズを網羅しなければならない。また、各フェーズをさらに詳細なアクティビティに分割して、そこで実施される作業と、入力および出力となるドキュメントを明確にしなければならない。

vii　項目間のトレーサビリティは明確に示さなければならない。

viii　開発者のコンピテンシを明確に示さなければならない。特に、IEC 61508 については、すべての開発者が理解していなければならない。

ix　IEC 61508 は対象範囲が極めて広い規格であるので、個別には適当でない要求事項もある。理由を明確にさえすれば、適合を免れる要求事項もあり得る。

⑤　本研究開発成果の国際認証機関の評価状況について

最終年度の調査では、開発成果物の一式を持参した上で、国際認証機関のレビューを受けた。特に、機能安全開発管理計画（FSMP）、安全コンセプト（SC）および、安全要求仕様（SRS）については、詳細な質疑応答を行った。その結果、これらの内容については十分に理解してもらうことができ、また、ほとんどの指摘事項を解決することができた。今後の対応が必要なものとしては、シーケンスモニタ機能によってどのようなカーネル故障がカバーされるかをより明確にすべき、との指摘事項があったが、安全分析を詳細に行うことで対応可能である。

その他の成果物については、比較的細かな指摘事項のみで、設計上の大きな修正が必要となるような指摘事項はなかった。参考までに、指摘事項の一部を以下に示す。

i　アーキテクチャ設計にはデータフローも示すこと。データフローからもテストケースを作成すること。

ii　オート変数は動的変数に該当するため、使用する場合には安全上の問題がない理由を明記すること。

iii　開発責任者の名前を FSMP に明記すること。

iv　RTOS および通信ミドルウェアの利用者がすべきことをすべて安全マニュアルにまとめること。

以上により、今回の成果物は、適合性評価において大きな問題はなく、指摘事項への対応を追加的に実施すれば、認証取得が十分可能な水準にあると考えられる。

第３章　全体総括

１．研究開発成果

本研究の開発成果は、当初計画と比較し保護機能開発を故障検出ライブラリ開発に変更するなど若干の修正があるものの全て目標に達成したレベルで完了した。

本研究での成果物は、オープンソースとしての公開準備が完了次第、NPO 法人 TOPPERS プロジェクトから一般公開することを予定している。

また、自動車制御用組込み OS の開発を担当した株式会社ヴィッツは、本研究成果の自社担当部位を利用し、国際認証機関である TUV_SUD からの機能安全認証取得に向けての活動を開始した。これは、本研究成果のレベルが、国際認証機関の認証可能レベルである事を証明するためであり、かつ、研究成果を用いた自社の機能安全事業立ち上げ活動を開始した。

各研究項目の成果・達成度等を以下に列記する。

①　機能安全に対応した自動車制御用組込み OS の開発

目標達成度：90%

得られた成果：機能安全対応 OS、機能安全認証用ドキュメント

特記事項：適合確認、監査の一部で条件付受容項目があり一部の作業残がある。未達理由は作業期間が短かったのみであり、問題となる課題は無い。対策として、本部位の担当は本研究副統括が所属する企業であり、継続作業を約束する。また、当該企業は、国際認証機関の認証評価を予定しているため、確実な対策が約束できる。

②　機能安全に対応した自動車通信ミドルウェアの開発と次世代車両例示アプリケーションの開発

目標達成度：CAN 通信 100%, LIN 通信 100%, FlexRay 通信 100%, 例示アプリケーション 80%

得られた成果：機能安全対応通信ミドルウェア(CAN/LIN/FlexRay)、ブレーキ機能アプリケーション、機能安全認証用ドキュメント

特記事項：各通信ミドルウェアは各ミドルウェア内で機能安全に特に必要となる部位の開発を完了させた。機能安全対応の通信ミドルウェアとして販売するには他の部位の対応も必要となるため、担当企業に開発の継続を依頼している。例示アプリケーションは、開発は終了したものの、検証および評価で一部作業残がある。この作業残もオープンソースとして一般公開するまでには対応する。

③　機能安全対策予備実験

目標達成度：100%

得られた成果：安全分析手法マニュアル（FTA,FMEA,HAZOP）、開発手法マニュアル(88 種類の手法; IEC61508-3 SIL3 HR 手法)、フォーマルメソッドマニュアル

(VDM, B, Z)、各実験結果レポート
特記事項 : 当初計画した分析/開発手法のマニュアル作成が完了した。これらの資料もオープンソースとして一般公開する予定である。

④　開発成果物の模擬認証
目標達成度：90%
得られた成果：各開発の認証に必要なドキュメント
特記事項 : 各開発の模擬認証は実施したが、あくまでも模擬であり国際認証機関の意見ではない。その点が本研究の最大の弱点であり、かつ、目標未達の原因でもある。そのため、株式会社ヴィッツは自社担当部位の認証取得活動を実施し、この模擬認証活動の妥当性を判断する。

⑤　第三者が再現可能な機能安全模擬認証対象機器の開発
目標達成度：100%
得られた成果：ブレーキ機能を含む電動カート
特記事項：対象機器の開発資料等もオープンソースとして公開を予定している。

本研究最終段階で、上記の開発成果を利用した実証実験を行なった。この実験では各開発成果の安全対策が正しく機能していることを、模擬認証対象機器を利用して確認した。確認事項としては、機能安全規格が要求する故障の検出や安全分析で求められた安全対策が実行されるかを確認した。

写真　1：カートを利用した実証実験

２．今後の課題及び事業化展開

(1)　今後の課題

①　本研究で調査/分析した機能安全対策方法が正しいか否かは、国際認証機関が責任を持って判断するものであり、内部関係者が判断できる内容ではない。そのため、本研究事業で国際認証機関からの認証取得活動が金銭的・制度的に出来なか

ったことが最大の課題である。

② この課題を解決するために、管理法人かつ統括副代表が所属する株式会社ヴィッツが研究成果を利用し、国際認証機関から機能安全認証を取得することを試みる。この活動により本研究の妥当レベルが明確となると共に、現在の隠れた課題が明確となり、同時に課題解決を行なう。

③ その他課題として、各研究項目での残作業が挙げられる。残作業は各社の事業化計画に沿って課題解決する。

(2) 事業化計画

各社の事業化計画は管理法人であっても指揮できないため、基本的に各社個別の事業計画を策定し、事業化を実現する。ただし、各社が協力することにより、より効果的な事業化が実現できる場合は、各社個別の事業計画に抵触しない程度に協力する。

基本的な考えとして、各開発成果物は開発機関の成果として事業化を検討する。すなわち、株式会社ヴィッツは自動車制御組込み OS を、株式会社サニー技研は CAN 及び FlexRay 通信を、東海ソフト株式会社は LIN 通信を製品化し、機能安全ソフトウェア部品事業を開始する。

一方、機能安全に関する業界での注目は高く、その事業化においては、機能安全対応ソフトウェア部品販売には留まらない。すなわち、安全を必要とする製品開発時に必要な機能安全開発能力、知識、ノウハウ等が重要であり、これらを利用したコンサルタント事業やソフトウェア開発受託等の事業化も実現可能である。

参画企業の秘匿事項にも関わるため、各社の事業化への取り組みは報告されていないが、事実、株式会社ヴィッツは研究途中である 2008 年より複数の産業機械メーカの機能安全対応製品の開発を支援しており、研究終了を前に機能安全に関する事業を実現している。また、本研究のアドバイザ企業からも機能安全に関連する調査・業務委託を受けており、事業化へは着実に進んでいる。

本研究のアドバイザ企業である川下企業群は、いずれも機能安全対応は避けることが出来ない業種であり、アドバイザ企業の多くは既に関連規格 ISO 26262 策定に関与し、機能安全対策に乗り出している。また、日本国内において機能安全規格やその対策において、本メンバほど精通している企業は少数である。

このことから、本研究のアドバイザ企業はもとより、研究外部である自動車メーカ、工作機械メーカ、医療メーカをはじめとして安全を必要とする製品開発企業との連携は強化されることが容易に予想される。

最後に、10 年後の日本国内において、機能安全の専門化・専門企業の 5 割は本研究メンバが占め、国内の機能安全事業の 7 割が本研究関連企業で占めていることが充分期待される。

付録

１．参考文献・引用文献

(1) IEC 61508-1, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 1: General requirements, 1998

(2) IEC 61508-2, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, 2000

(3) IEC 61508-3, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 3: Software requirements, 1998

(4) IEC 61508-4, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 4: Definitions and abbreviations, 1998

(5) IEC 61508-5, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 5: Examples of methods for the determination of safety integrity levels, 1998

(6) IEC 61508-6, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 6: Guidelines on the application of AS 61508.2 and AS 61508.3,2000

(7) IEC 61508-6, Functional Safety of electrical/electronic/programmable electronic safety-related system – Part 7: Overview of techniques and measures, 2000

(8) IEC 61784-3, Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions, 2007

(9) ISO 11898-1, Road vehicles -- Interchange of digital information -- Controller area network (CAN) for high-speed communication, 1993

２．専門用語の解説

専門用語	解　説
FTA	フォルトツリー解析（フォルトツリーかいせき、Fault Tree Analysis）とは、故障・事故の分析手法 望ましくない事象に対し、その要因を探るトップダウンの解析手法を特徴とする。
FMEA	FMEA（Failure Mode and Effect Analysis）（意味：故障モードとその影響の解析）は、 故障・不具合の防止を目的とした、潜在的な故障・不具合の体系的な分析方法
HAZOP	Hazard And Operability Study の略 危険シナリオ分析手法の一つで　化学プロセスにおける複数の独立した事象が複雑に絡む故障を取り扱うために開発された手法

VDM	VDM（Vienna Development Method）は、IBM のウィーン研究所で 1960 年代から 70 年代にかけて開発された形式手法
Z	Z 言語（ぜっどげんご）は、Z 記法（ぜっどきほう）ともいい、形式仕様記述言語であり、コンピュータシステムの記述とモデリングを行うために使われる
B	B-Method とは、AMN（Abstract Machine Notation）という仕様記述言語（兼プログラミング言語）を中心とした形式手法に基づいたソフトウェア開発手法である
SIL	Safety Integrity Level の略であり、安全度水準と訳される。IEC61508 では求められる安全度を示し、SIL 1～SIL4 までが規定されている
API	Application Program Interface の略。あるプラットフォーム(OS やミドルウェア)向けのソフトウェアを開発する際に使用できる命令や関数の集合を示す
W/D	ウォッチドッグタイマー（watchdog timer）は、コンピュータのハードウェア時間計測器である。メインのプログラムがハングアップなどの不正な状態に陥ってしまい規則的なウォッチドッグ操作(「犬をなでる」とも呼ばれる「サービスパルス」の書き込み）が行なわれなかった（タイムアウト）場合に、システムを正常動作に戻すことを目的として利用される

引用：

http://blog.isovocabulary.com/16_riskmanagement/hazop/http://e-words.jp/w/API.html

Wikipedia