機能安全対応 TOPPERS 開発成果の開発状況報告

株式会社ヴィッツ
服部博行

謝辞および前提条件

TOPPERSから公開する予定の機能安全対応RTOSおよび車載通信ミドルウェアは，経済産業省・(独)中小企業基盤整備機構の戦略的基盤技術高度化支援事業の採択テーマとして実施中の「機能安全対応自動車制御PFの開発」の成果を利用する予定である。

本資料および開発等に関し、プロジェクトのメンバならびにアドバイザ各位に感謝する

メンバ組織

(株)ヴィッツ、(株)サニー技研、東海ソフト(株)

名古屋大学(NCES)、産業技術総合研究所(CVS)

名古屋市工業研究所、北海道立工業試験所

アドバイザー組織

トヨタ自動車(株)、アイシン精機(株)、(株)東海理化

アイシン・エイ・ダブリュ(株)、(株)ルネサステクノロジ

(株)豊通エレクトロニクス

「機能安全対応自動車制御PF」研究プロジェクトの概要

目的

機能安全規格(IEC 61508) のSIL 3の認証が取れるレベルのRTOSと車載ネットワークミドルウェアを開発

予算

経済産業省 戦略的基盤技術高度化支援事業の採択事業として実施

2006年12月より3ヶ年間で研究実施

認証計画

この研究プロジェクト内で IEC61508 の認証を得ることはできない。

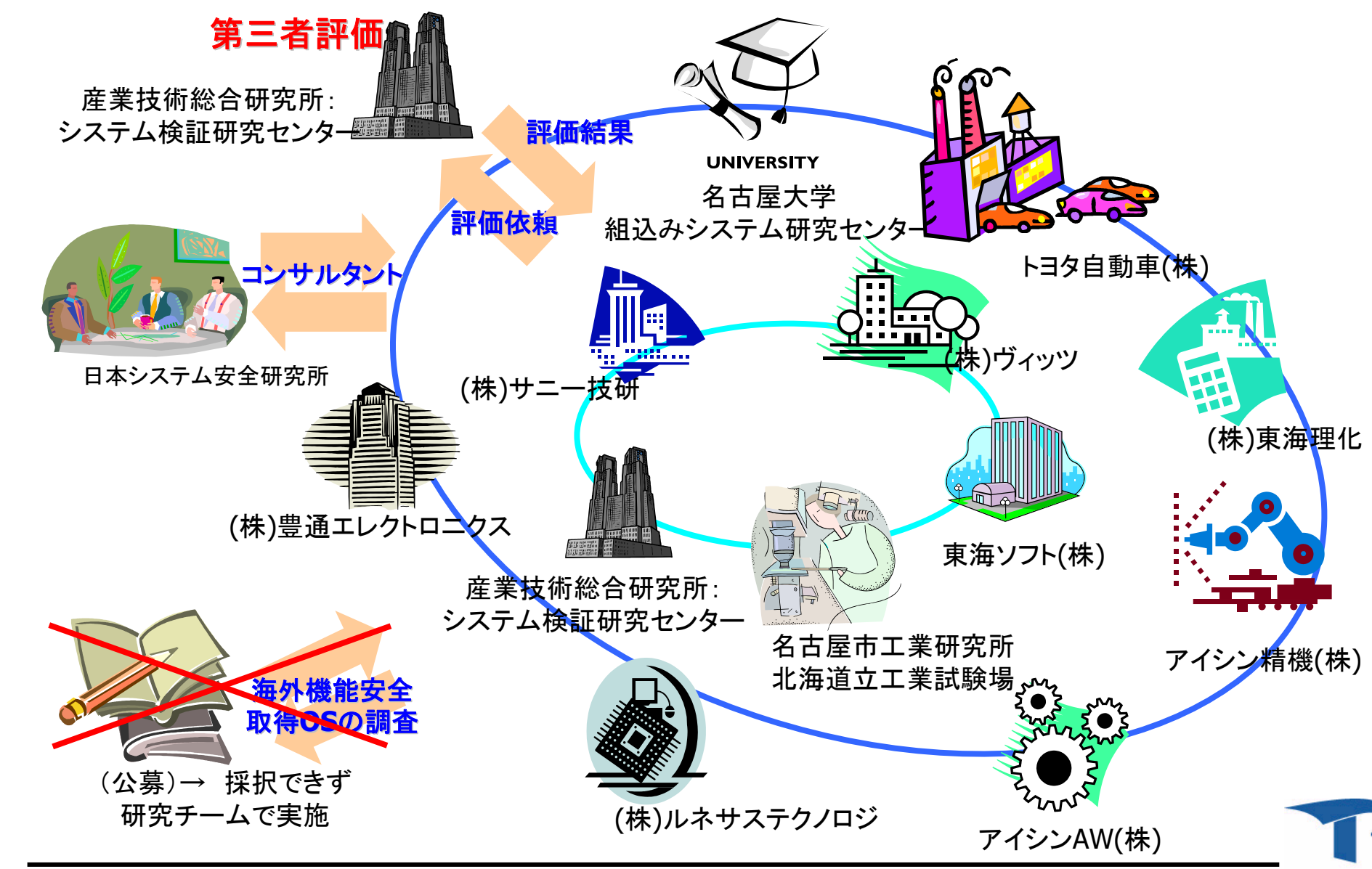
認証には、1製品あたり数千万規模の認証費用が必要で、研究予算で賄うことができない。

研究を通じて、認証費用の捻出方法を検討中

この研究プロジェクト成果をTOPPERSから公開する予定です

TOPPERS

開発体制 (川下産業と川上産業のコンソーシアム)



機能安全とは？

機能安全 (Functional safety)

新しい用語

本質安全と対比する用語

（(株) 日本機能安全　田邊安雄）

本質安全と機能安全

本質安全

機械が人間や環境に危害を及ぼす原因そのものを低減あるいは除去する

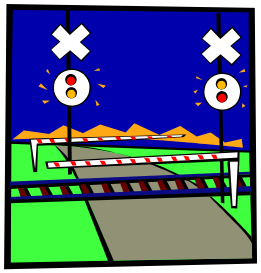
鉄道を例にすると、立体交差にすれば、踏切を渡って事故に遭遇する可能性はない

機能安全

機能的な工夫(安全を確保する機能) により極力安全を確保する

鉄道を例にすると、踏切の警報機や遮断機

安全を確保する機能を安全機能(safety function)，安全機能を実現するシステムを安全関連系(safety-related system) と呼ぶ



参考：NECA 技術委員会報告第3の波「機能安全」の概要

機能安全の定義

機能安全の定義

「機能安全とは入力に対して正しく動作するシステムや機器に依存する全体安全の一部である。機能安全は要求された機能が機能するとき、達成される」

(IECのWEBサイトでの定義)

上記定義から、

製品を対象としている （しかもシステム機器全体で考える）

安全に対する要求が必要である。安全に対する要求は“本来”抜けがあってはいけない

安全に対する要求が“しっかり”定義され、その定義機能が正しく機能（作られている = 信頼性のある品質で作られている）しているならば、安全は担保される

ならば、

安全性と信頼性の関係を考える必要がある

言葉ではなんとなく理解できるけど、しっくりこない

システムの安全性と信頼性

システム信頼性:

機能単位が要求された機能を与えられた条件のもので、与えられた期間実行する能力(JIS X 0014)

システム安全性:

システムが規定された条件のもとで、人の生命、健康、財産またはその環境を危険にさらす状態に移行しない期待度合い(JIS X 0134)

だとしたら、

信頼性:

「要求された機能」を満たすこと。要求された機能を満たしていても人命等を危険にさらす場合はある。信頼性は安全性ではない。

安全性:

機能を満たして無くても、人命等を危険な状態さらさないなら、安全である。

例)動かない車 (これは車と呼べるかは別の議論

安全機能と安全要求分析　～機能安全定義のまとめ～

機能安全の考え方

機能により，「人の生命，健康，財産またはその環境を危険にさらす状態に移行しない」ようにすること

安全性の確保とは？

安全性を確保するために必要な機能(安全機能) が定義できれば，後は，信頼性を確保すればよい

機能安全対応で最も重要なこと

安全性を確保するために取るべき手段(安全機能を含む)を抽出するための分析作業

これに成功すれば，後は信頼性を確保すればよいという意味で，機能安全実現に向けての最も重要な(かつ難しい) 作業

安全分析の手法例

FTA （Fault Tree Analysis ）

障害となる事例を元に、その障害が発生する要因を抽出する

抽出した要因の発生率を検討して、対策方法を求める

例） ブレーキが利かない　→　ブレーキオイルが無い・・・

FMEA (Failure Mode and Effect Analysis)

システムを構成している要素を対象とし、考えられる故障と影響を抽出する

故障の発生頻度と影響度から対策の可否や方法を検討する

例) ソフトウェアならフローチャートを用いると分かりやすい

HAZOP (Hazard and Operability Study)

対象となる機能の期待される振る舞いに対して、ガイドワードと呼ばれる事象を当てはめて、原因と影響を抽出する

故障の発生頻度と影響度から対策の可否や方法を検討する

研究プロジェクトの大きな壁

分析手法の対象

FTA,FMEA,HAZOPは、基本的にシステムを対象とした分析手法

システムが対象であれば、安全分析は可能

研究の対象

RTOS , CAN/LIN/FlexRay通信ミドルウェア

いずれもコンポーネント（部品）であり、利用されるシステムは特定できない

→　使われ方、問題発生時の影響などがわからない

どうやって分析するか？

複数のシステムを分析し、コンポーネントへの安全要求を一般化する

コンポーネント単体での分析方法を検討する

規格から考えるコンポーネント単位の機能安全

機能安全規格の対象範囲

- 対象はシステム単位 (コンポーネント単位では考えられていない)
- コンポーネント単位での対応はメリットが多い（はず）

どんな機能があれば、機能安全コンポーネントと言えるのか？

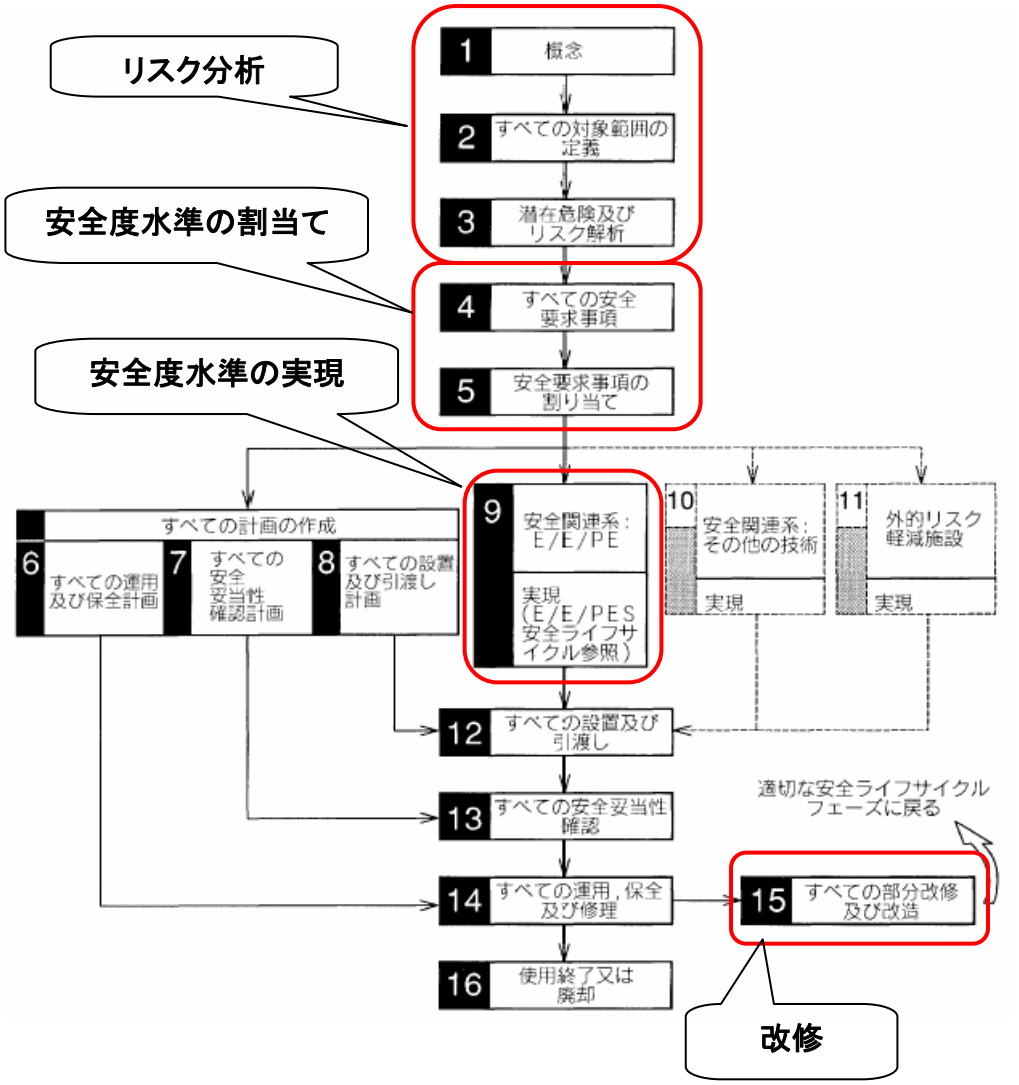
- 規格には、必要な機能に関する記述はない
- システムが要求する安全機能をコンポーネントを利用して満たせればよい
  - コンポーネントもしくはアプリで実現できればよい （たぶん）
  - コンポーネントが対応する機能を明確する （たぶん）
  - アプリで実現が困難な機能はコンポーネントで実現 （たぶん）

規格から考えられる機能安全対策

- **IEC61508** に記載されているライフサイクル、開発モデル、開発手法を遵守して開発するしか手はなさそう

本研究でのアプローチ　～全安全ライフサイクル～

対象はソフトウェア開発なので、ソフトウェアコンポーネントの機能安全対策を考える



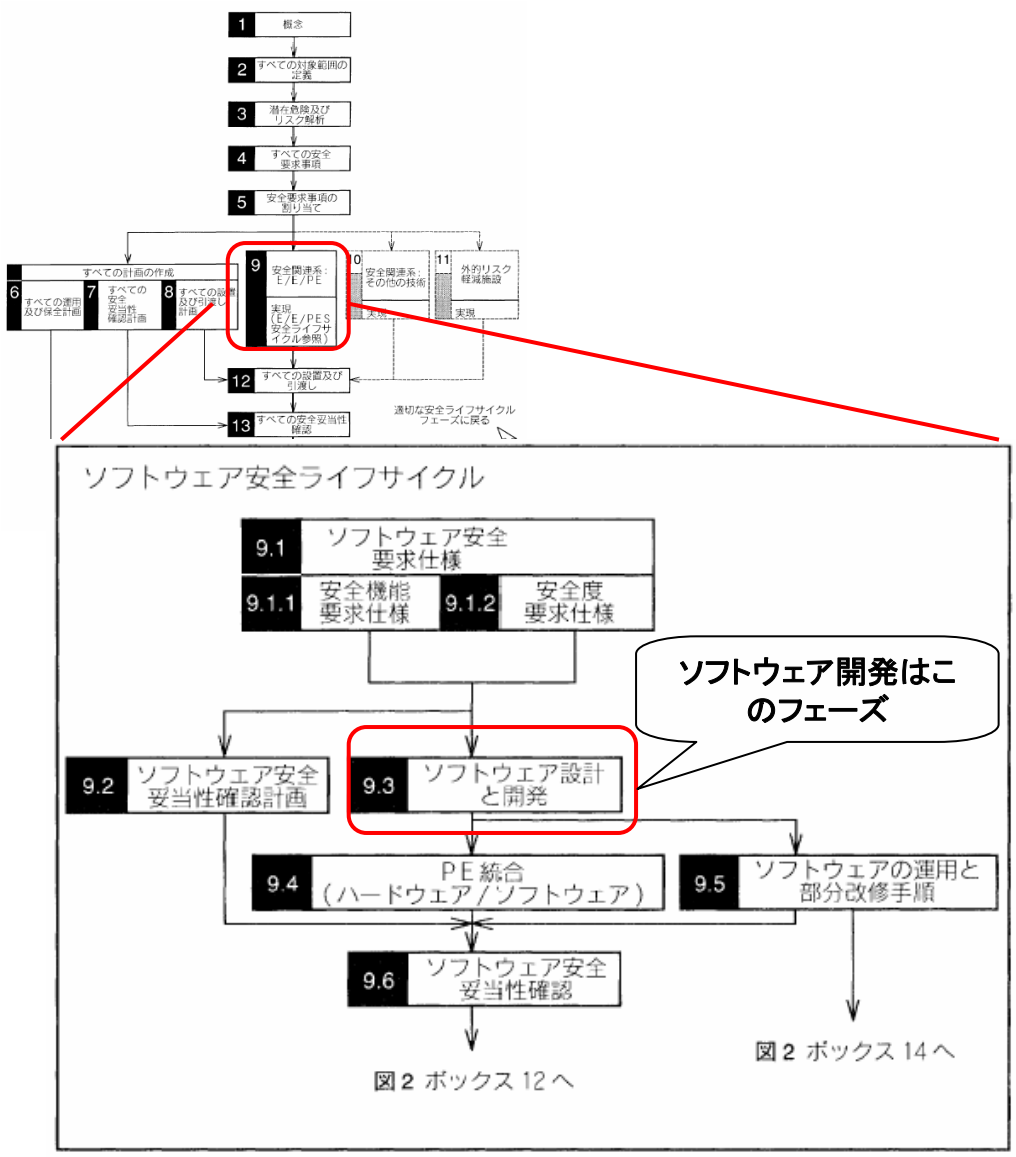
ソフトウェア開発は9の実現フェーズにて実施する

そのため、実現に必要な入力フェーズは機能安全対応のソフトウェア開発には必要な作業である

通常、実現フェーズの入力はソフトウェア発注先の仕事となる

JIS C 0508-1 より引用

本研究でのアプローチ　～ソフトウェアライフサイクル～

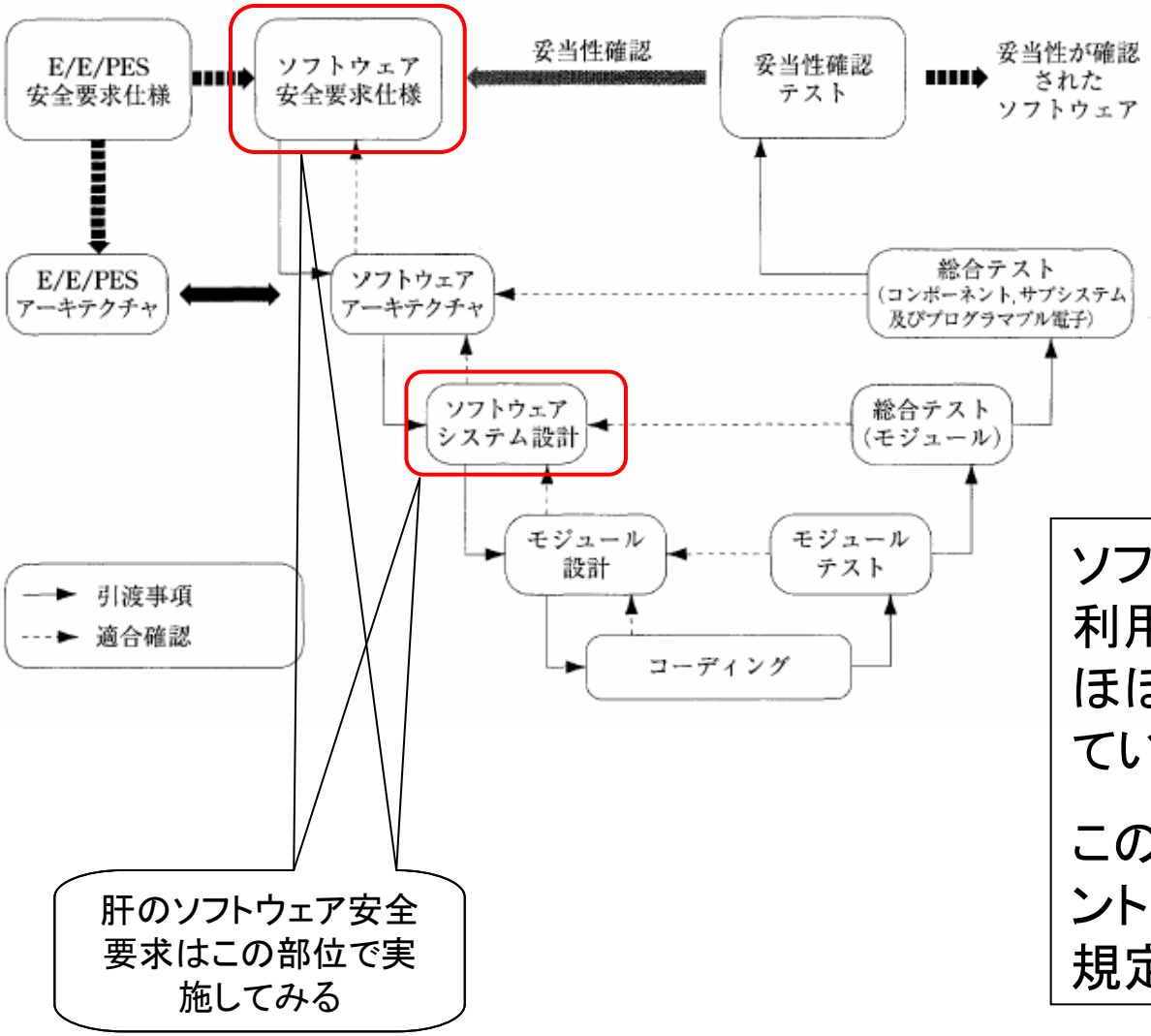


ソフトウェア開発は9.3のソフトウェア設計と開発フェーズにて実施する

このフェーズは、IEC61508-3にて規定されており、開発のV字プロセス、開発手法、開発ドキュメントなどが細かく規定されている

JIS C 0508-1 より引用

本研究でのアプローチ　～V字プロセス～



ソフトウェア開発で一般的に利用されているV字プロセスとほぼ同じプロセスが規定されている。

このプロセスに入出力ドキュメントや各工程での開発手法が規定されている

JIS C 0508-3 より引用

本研究でのアプローチ　～安全要求分析～

コンポーネント単位の安全分析

考えられる方法は2種類

・複数のシステムを分析し、コンポーネント単位の安全分析を一般化する

ヴィッツ製電動カードを利用し、システム分析を実施

FTA,FMEA,HAZOPの手法を利用

結果

1システムの分析で膨大な分析時間が必要

システムからコンポーネント単位分析に到達するまで時間がかかりすぎる

このアプローチは実現できない

・コンポーネント単位での分析方法を検討する

英国 **York**大学のコンポーネント分析論文を参考に

自動車向け**RTOS**特性を追加した分析を実施

結果

ソフトウェア**HAZOP**手法に似ているが、コンポーネント単位での分析が可能と判断

本研究でのアプローチ　～その他のプロセス関連～

開発ドキュメント

規格が要求するドキュメントおよび内容を検討し、必要項目を網羅したサンプルドキュメントフォーマットを規定

開発手法

規格が紹介している開発手法の目的、対応項目などを検討し、手法利用時のマニュアルを作成

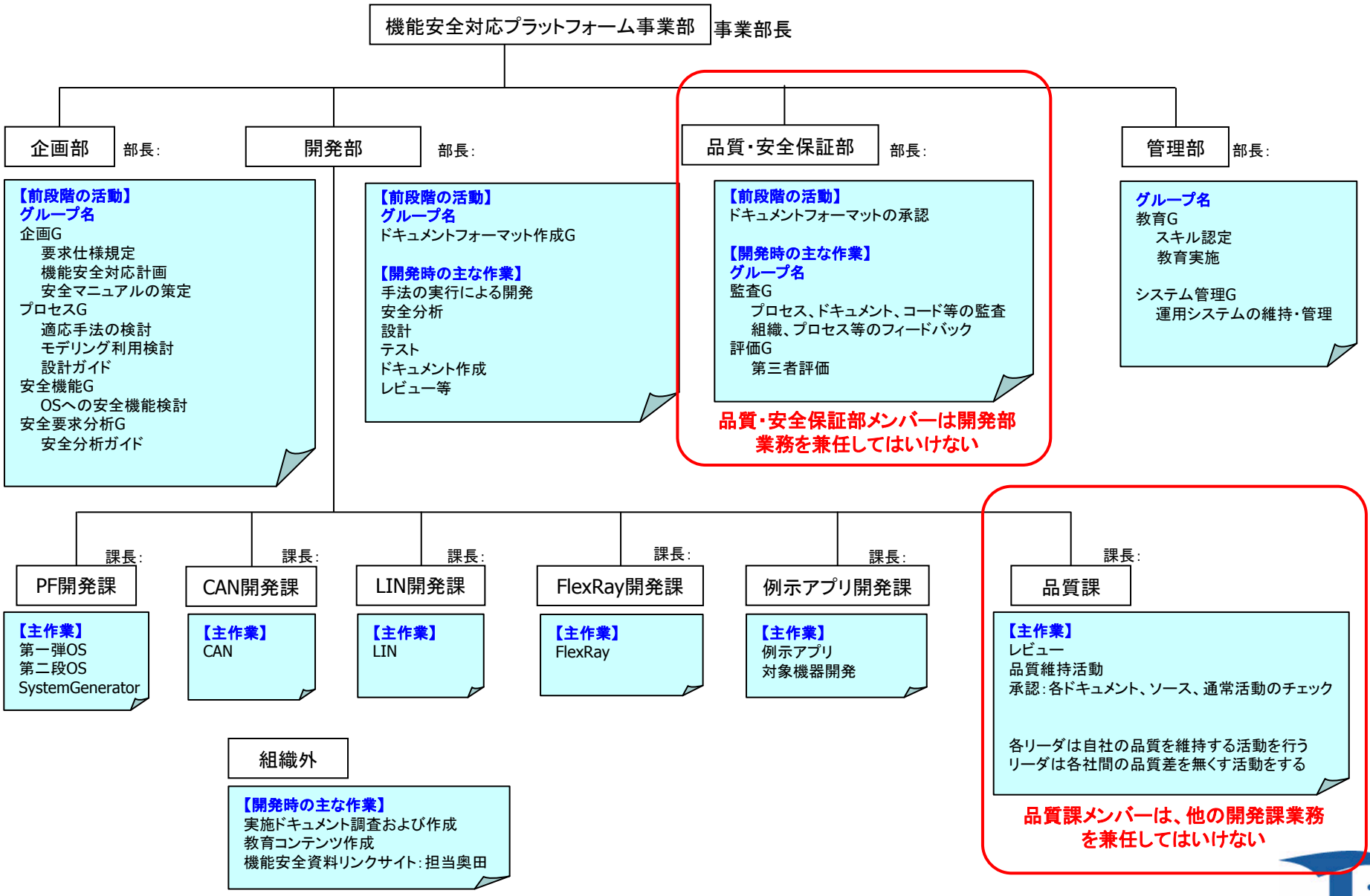
機能安全開発マニュアル

機能安全開発を行うに必要な管理方法をまとめた開発マニュアルを作成

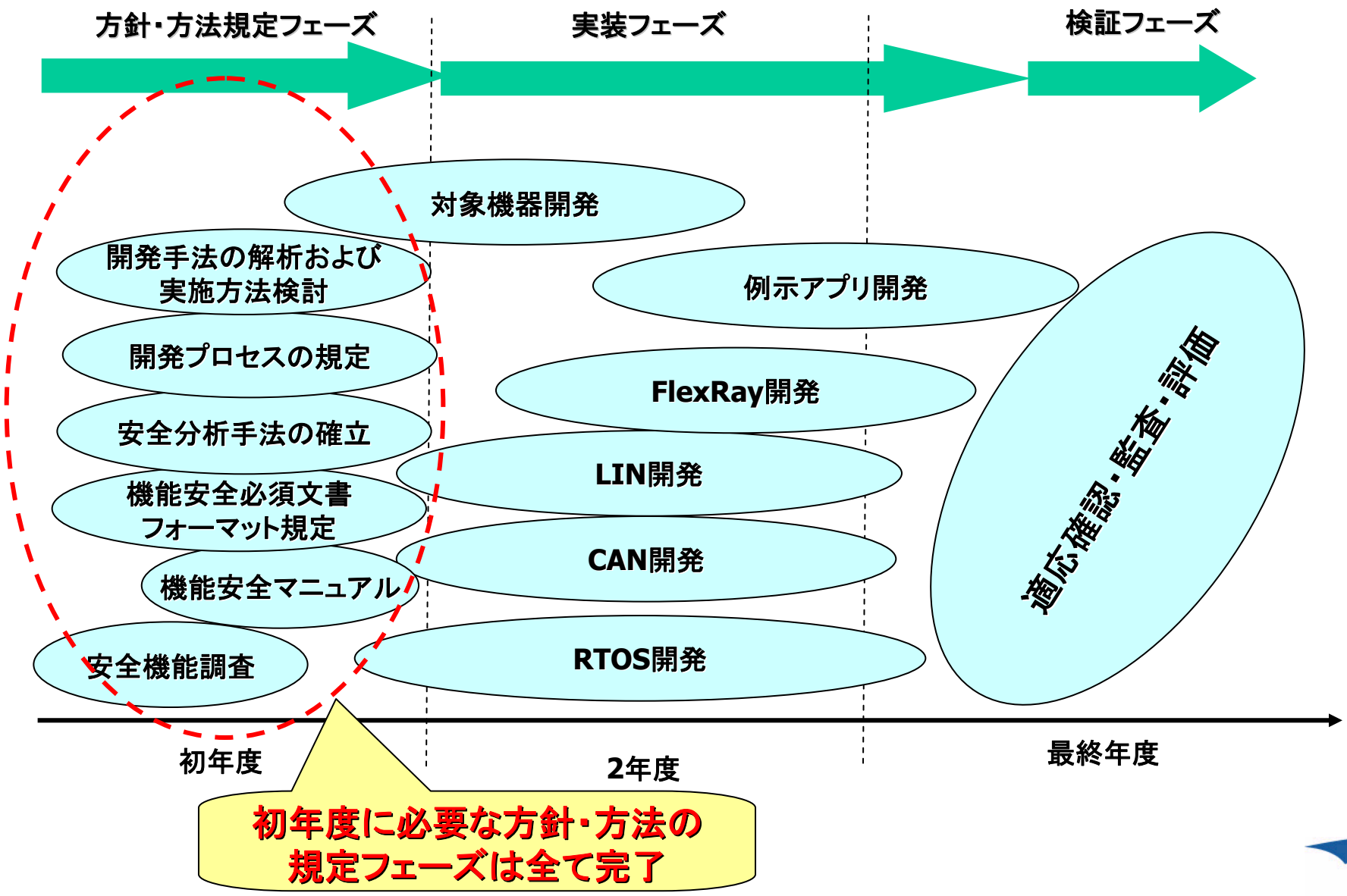
仮想組織の策定

規格が要求する組織と管理をまとめ、参考となる組織例を規定
また、本研究プロジェクトは複数社で開発するため、会社の壁を越えた仮想組織を策定して開発を実施

本研究でのアプローチ　～仮想組織～



本年度の目標と実績


方針・方法規定フェーズ
実装フェーズ
検証フェーズ
対象機器開発
開発手法の解析および
実施方法検討
例示アプリ開発
開発プロセスの規定
FlexRay開発
安全分析手法の確立
LIN開発
機能安全必須文書
フォーマット規定
CAN開発
機能安全マニュアル
適応確認・監査・評価
安全機能調査
RTOS開発
初年度
2年度
最終年度
初年度に必要な方針・方法の
規定フェーズは全て完了

開発状況報告

参考となる事例が存在しない中、本研究は機能安全規格の解釈から実施し、本年度の最大かつ唯一の目標である機能安全規格対応方法を独自に導き出すことができました。

これは業界内外を通じ、非常に価値がある成果である考えています。

3年後に、IEC61508 SIL3 が取得できるレベルのOSと通信ミドルウェアを開発し公開するとともに、取得に必要な各種ドキュメントを公開したいと思います

これからもTOPPERSプロジェクトを応援してください

ご静聴ありがとうございました

本内容についてのご質問は下記にお願いします
株式会社ヴィッツ
組込みソフトウェア開発部
Tel: 052-220-1218
服部博行
hat@witz-inc.co.jp