



機能安全対応自動車制御用 プラットフォームの開発報告

Embedded Technology 2009

株式会社ヴィッツ

水野智仁

<http://www.witz-inc.co.jp>

mailto:users_support@witz-inc.co.jp

- 機能安全とは？
- 機能安全対応自動車制御用プラットフォームの開発について
- 成果報告
- 開発で得たこと
- 機能安全ソリューションの紹介

機能安全とは？

本質安全

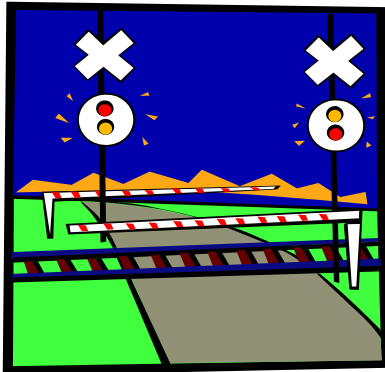
機械が人間や環境に危害を及ぼす原因そのものを低減あるいは除去する

例：踏切を立体交差にすれば、踏切を渡って事故に遭遇する可能性が無くなる

機能安全

機能的な工夫(安全を確保する機能;以降、安全機能)を導入して許容できるレベルの安全を確保する

例：踏切の警報機や遮断機(警報機や遮断機がついていても絶対的に安全とは言えないが、許容できるレベルの安全は確保している)

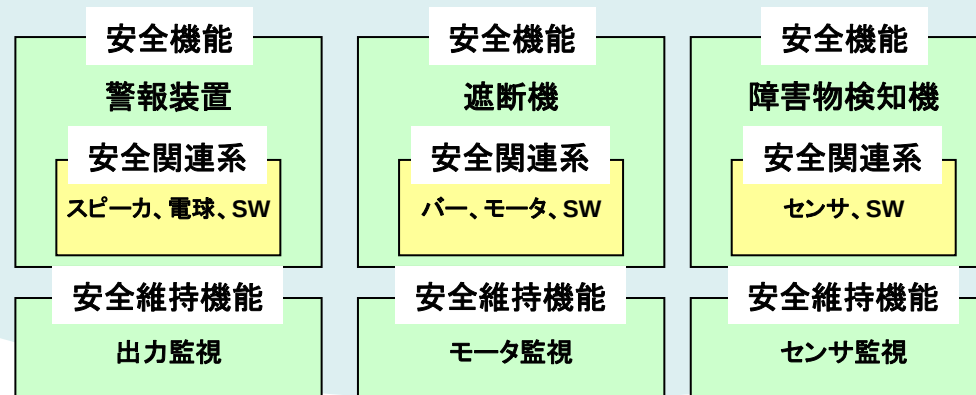
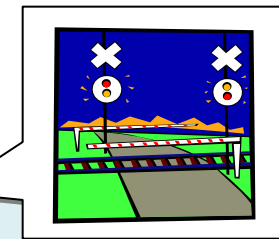


参考:NECA 技術委員会報告第3の波「機能安全」の概要

- **機能安全** (Functional safety) :
 - 機能そのものを指すわけではなく**考え方を示す**用語
- **安全機能** (Safety function) :
 - 安全得るための機能
- **安全関連系** (Safety-related system) :
 - 安全機能を実現するシステム (要素群を含む)
- **安全維持機能** (Safety integrity functions) :
 - 安全関連系の構成要素が正しく動作するための機能
 - (すなわち安全機能が正しく動作を継続するための機能)

機能安全

警報装置・遮断機による注意喚起と進路変更により安全を考える



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)

→「要求された機能を満たすこと」 要求機能を満たしても安全とは限らない

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)

→「危険な状態に移行しないこと」 機能要求を満たしているは不問

名古屋大学 高田広章

信頼性と安全性は同じでない

・ 機能安全規格(IEC 61508)

- IEC61508は全ての機能安全規格のベース
- 電気・電子・プログラマブル電子系全般を対象
- 7部構成

第1部 一般要求事項

第2部 電気・電子・プログラマブル電子 安全関連系に関する要求事項

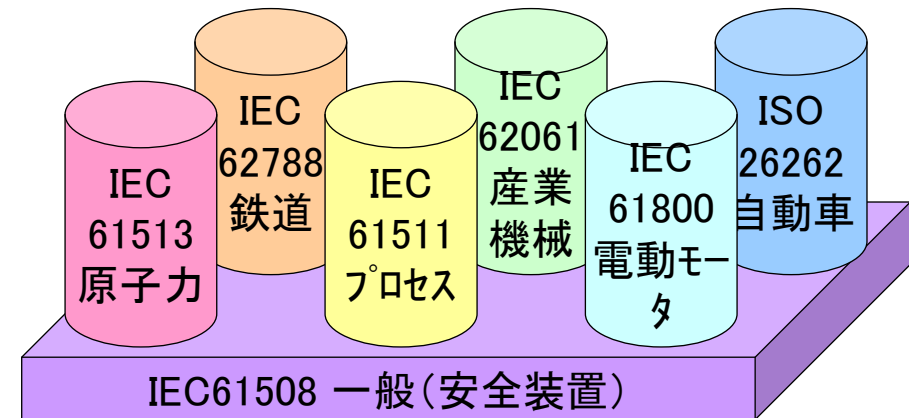
第3部 ソフトウェア要求事項

第4部 用語の定義および略語

第5部 安全度水準決定方法の事例

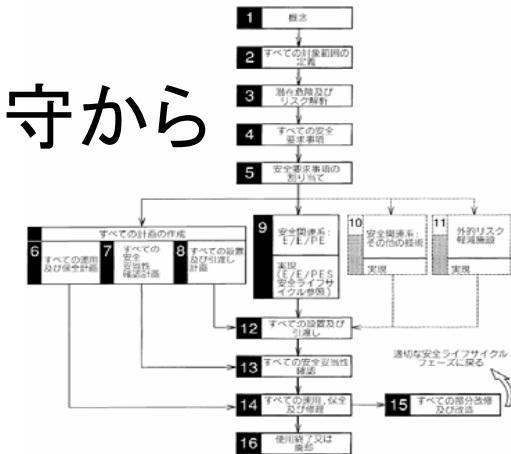
第6部 第2部及び第3部の適用指針

第7部 技術及び手法の概観



IEC 61508と派生規格

- 製品安全のコンセプト
- 安全ライフサイクルの規定
 - 製品概念、安全分析、設計製造、運用保守から改修廃却に至るまで規定
- 根本原因(人・組織・技術)の管理



技術原因

- 表面的な安全活動
- 根本的な設計欠如
- 情報の不足
- 変更に対する評価の失敗
- 有効でないリスク管理

人的原因

- 知識、技術不足
- 情報伝達ができない
- 細部への注意不足
- 安全に関する信念が弱い
- コミュニケーション下手

組織原因

- 責任と権限の分散
- 独立性の欠如
- 安全担当部門の低い地位
- 情報伝達経路の限定
- 貧困な情報の流れ



「機能安全対応自動車制御用プラットフォームの開発」 研究内容

- 背景

- 欧州の機能安全規格が世界的規模で義務付けが検討されている。
- 日本のものづくり産業に対する影響が非常に高い。

- 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する
 - サンプルアプリケーションで機能安全を実現
 - ソフトウェアをオープンソース化
 - 開発過程をドキュメント化し、ドキュメントを公開

- 開発成果物

- 機能安全対応自動車制御用OS、機能安全対応CAN/LIN/FlexRay通信ミドルウェア及び認証可能な各種ドキュメント
- X-by-Wire電動カートを例にした制御アプリケーション
- 機能安全規格関連ドキュメント

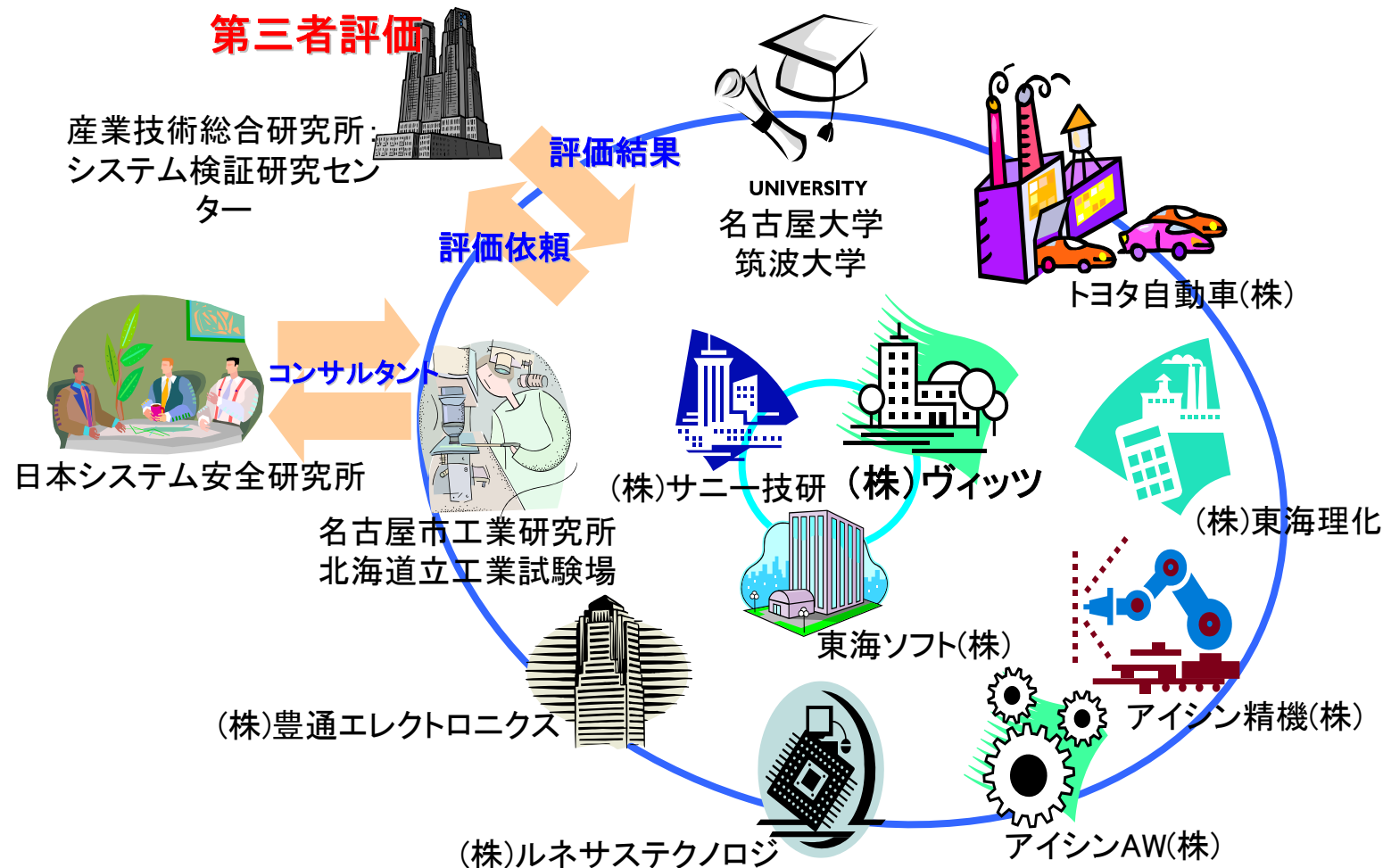
- 予算

- 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

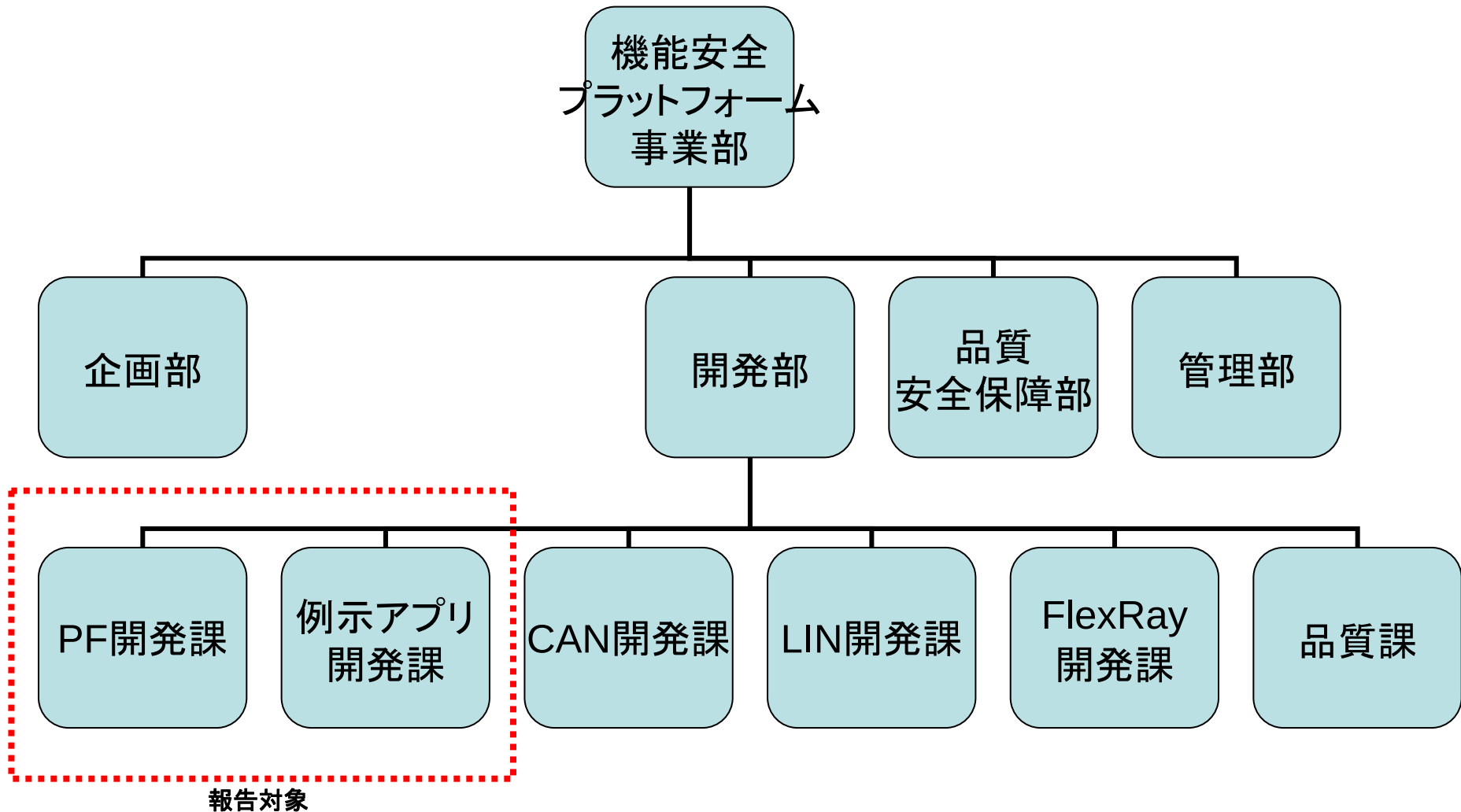
- 認証計画

- 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。

プロジェクト体制：産官学連携



- 仮想組織体制



本研究でのアプローチ

•ソフトウェア開発前段階でのアプローチ

- 機能安全開発マニュアルの作成（6.2.1の管理:実施計画書の共通部を抽出）
 - 安全度水準の規定、ソフトウェア開発プロセスの規定
 - 各プロセス工程での作業内容の規定と実施マニュアルの策定
 - 安全分析手法マニュアル作成、IEC61508が推奨する各種手法のマニュアル作成
 - 構成管理方法の検討と実施マニュアルの作成
 - 作業実施者のスキル判定と教育方法の検討
- 機能安全開発の対象と範囲の規定
- IEC61508が要求する文書の規定と文書フォーマットの作成

•ソフトウェア開発中のアプローチ

- ソフトウェアコンポーネント単位での機能安全同定検討
- 故障率とソフトウェアの関係
- OSの開発、通信ソフトウェアの開発、例示となるアプリケーションの開発

機能安全規格調査
機能安全対策調査

調査
内容

機能安全開発プロセスの規定
ソフトウェアの安全分析手法の確立

ノウハウ

手法
プロセス

開発対象に求める
安全機能の開発

安全
機能仕様

開発過程のドキュメント作成
機能安全教育コンテンツの開発

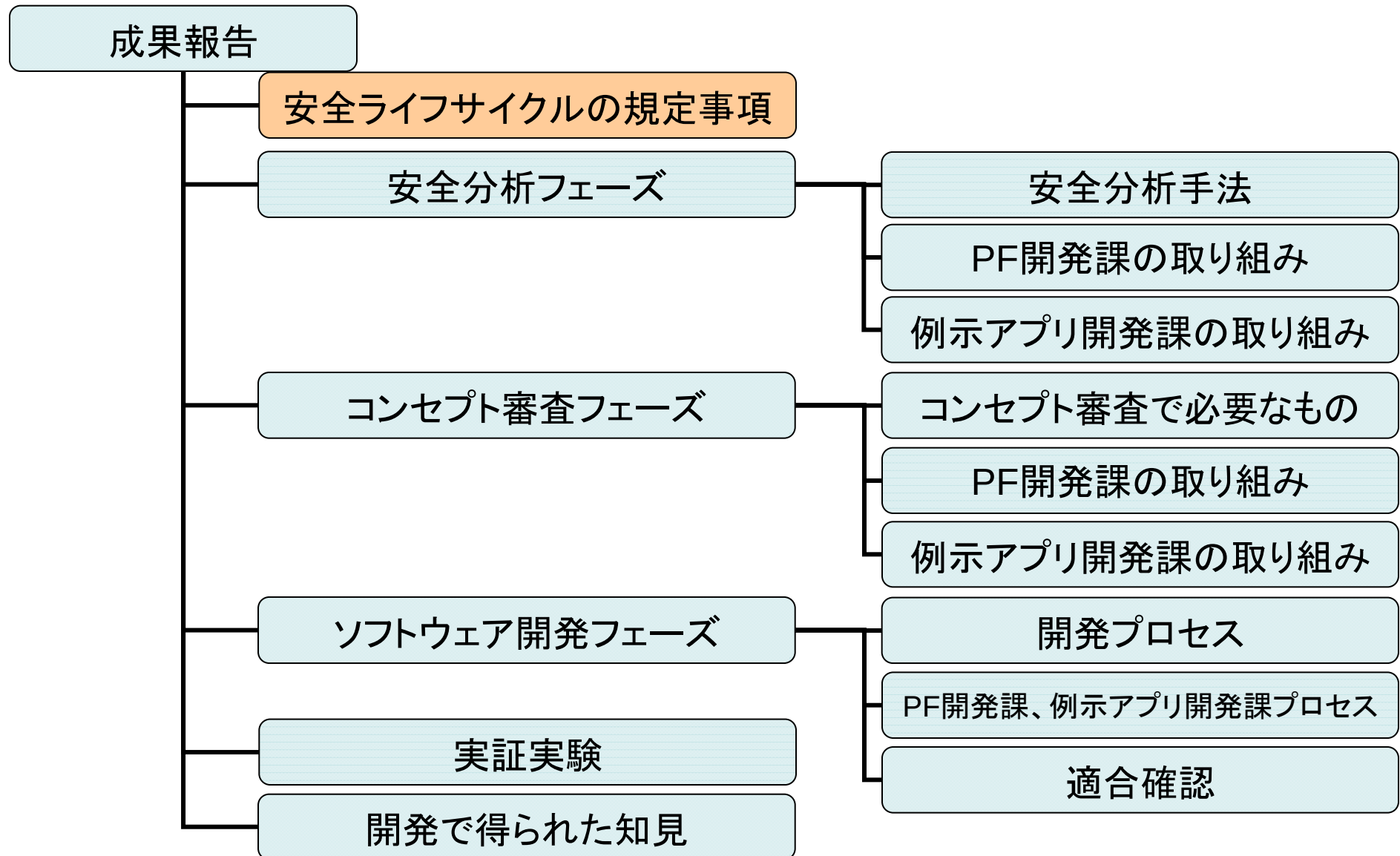
ノウハウ

機能安全対応ソフトウェアの開発
機能安全対象機器の開発

株式会社



「機能安全対応自動車制御用プラットフォームの開発」 成果報告



安全ライフサイクルの規定事項

開発対象の**範囲を決定**し、潜在危険及びリスク解析の**範囲を定義**することを目的とする。

他の安全ライフサイクル業務が十分に実施できるように、開発対象の概要及び、運用方法、又は利用について一定の水準の**理解を図る**ことを目的とする。

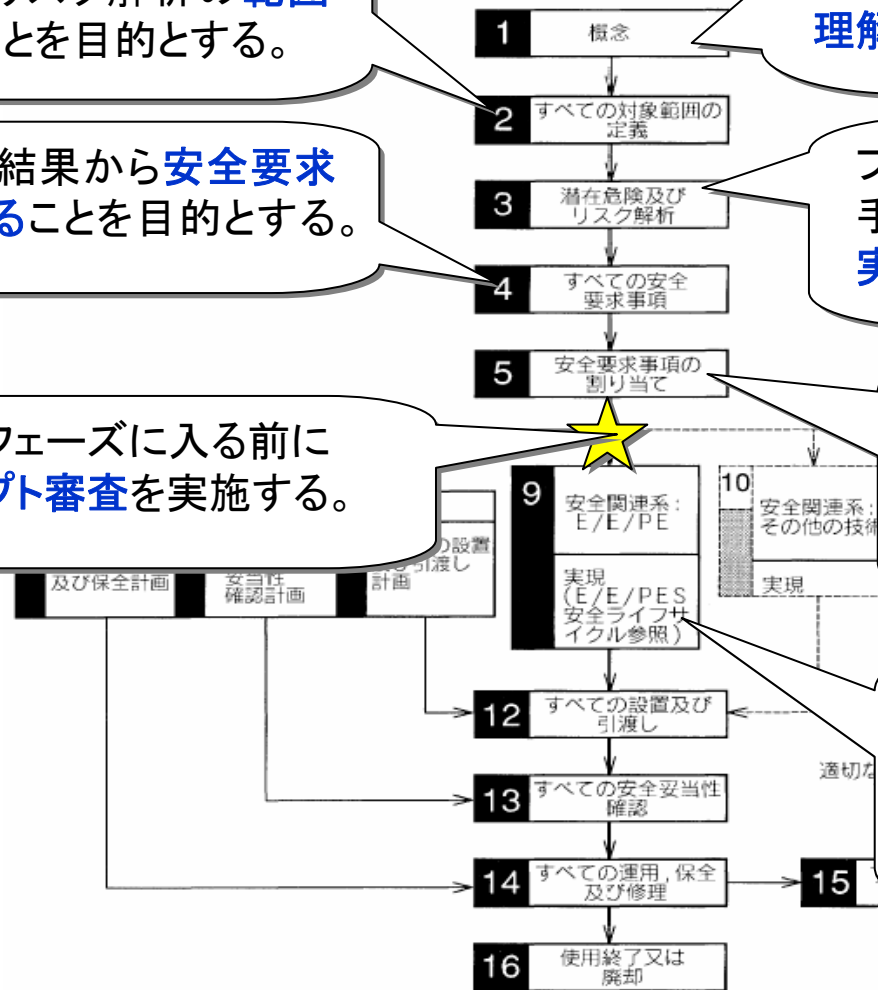
安全分析の結果から**安全要求事項を求める**ことを目的とする。

プロジェクトで規定している安全分析手法の作業手順に従って**安全分析を実施する**ことを目的とする。

開発フェーズに入る前に**コンセプト審査**を実施する。

ソフトウェア、ハードウェアに対して**SILを割り当てる**ことで、システム全体に対してSILを割り当てる必要がある。

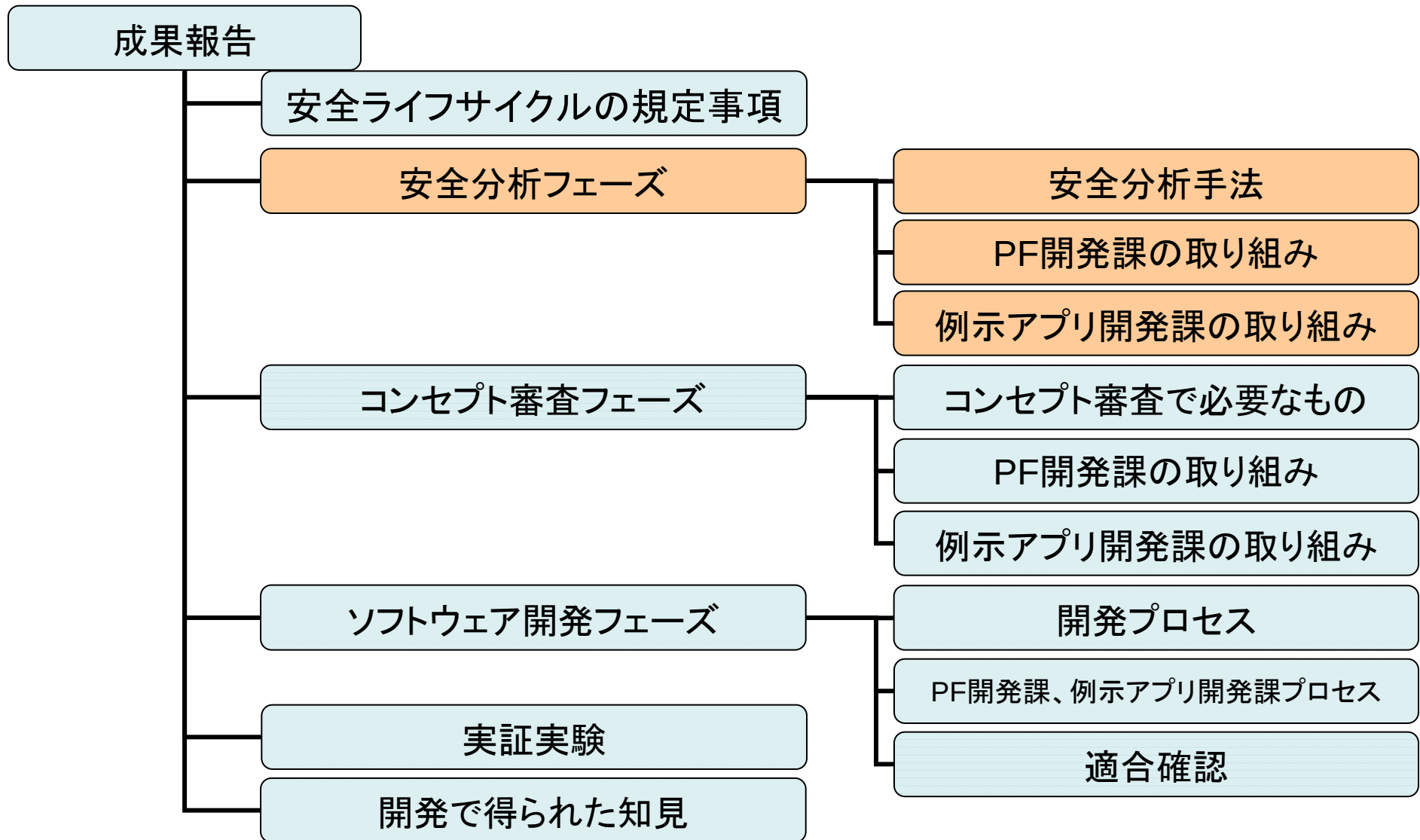
ソフトウェア安全ライフサイクルに従い開発を実施する。**ソフトウェアの開発**はこのフェーズでほぼ完了



JIS C 0508-1 より引用

株式会社ヴィッツ

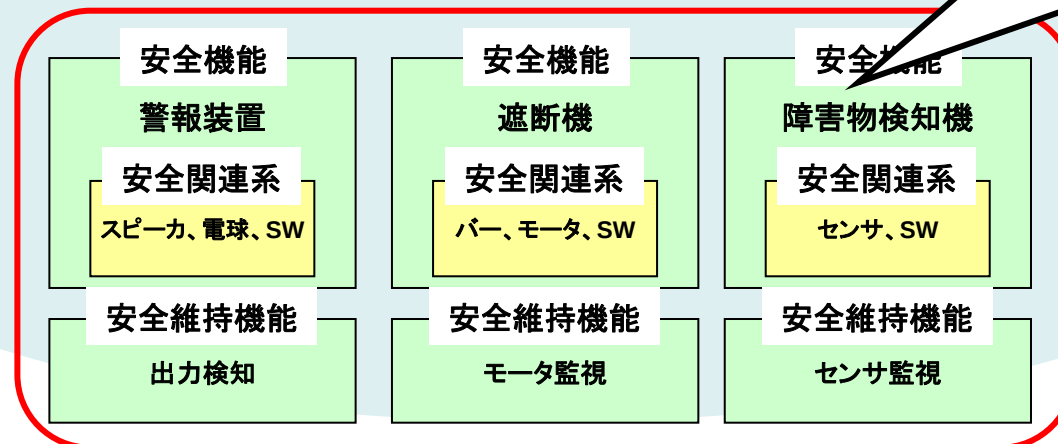
Embedded Technology 2009



- 安全性を確保するために**取るべき手段**を抽出するための**分析作業**
- 機能安全実現に向けて最も**重要**かつ難しい作業
- 分析手法例: **FTA、FMEA、HAZOP**

機能安全

警報装置・遮断機による注意喚起と進路変更により安全

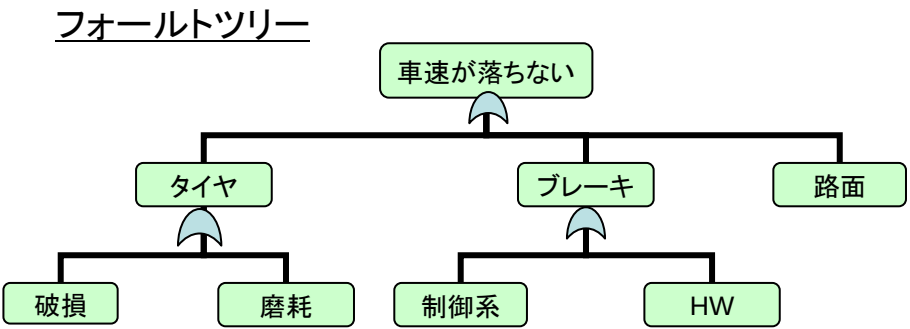


この部位である“安全機能”、
“安全維持機能”を安全分析作業
から**抽出**する

FTA (Fault Tree Analysis)

障害となるトップ事例を元に、その障害が発生する要因をフォールツリーを用いて抽出する。抽出した要因の発生率を検討して、対策方法を求める。

トップダウンで解析する。



FMEA (Failure Mode and Effect Analysis)

システムを構成している要素の故障モードを挙げて、システムに対する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。

ボトムアップで解析する。

FMEAワークシート

アイテム	機能	故障モード	推定原因	故障の影響		検知方法	故障等級	特記事項
				サブシステム	システム			

HAZOP (Hazard and Operability Study)

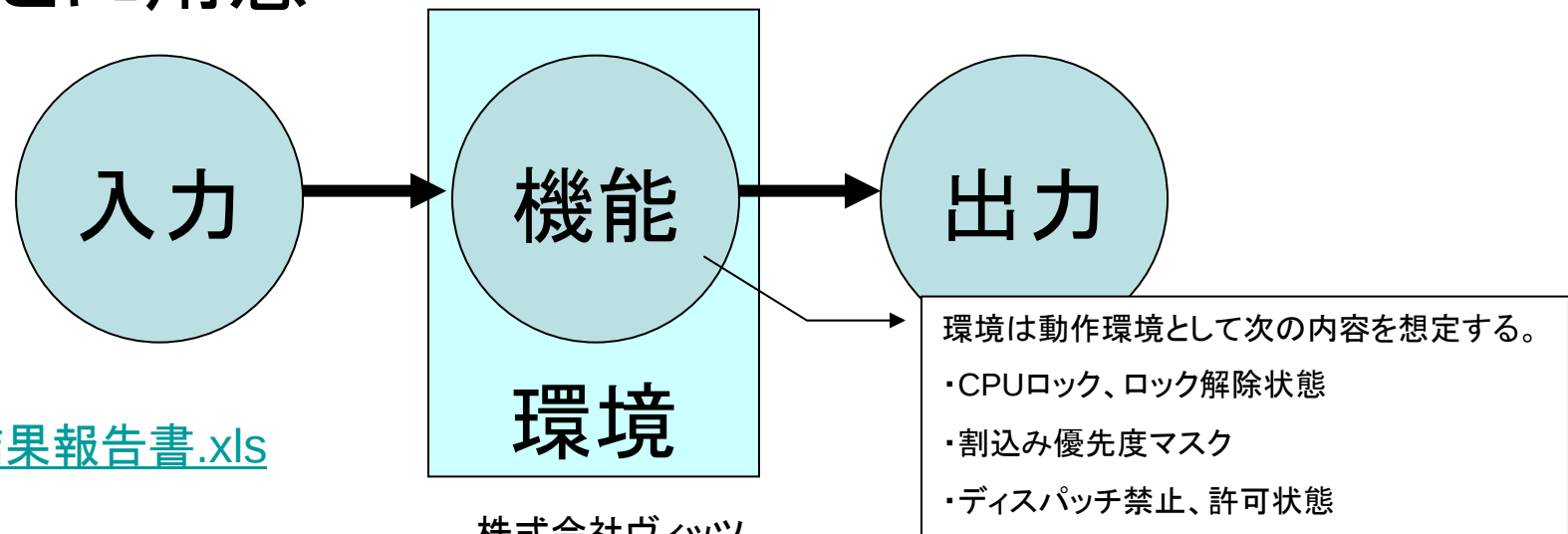
対象となる機能の期待される振る舞いに対して、ガイドワードと呼ばれる事象を当てはめて、原因と影響を抽出する。

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

HAZOPガイドワード

No, More, Less, As well as, Part of, Reverse, Other than, Later, Higher, Lower, ,,,

- 分析対象:カーネル基本機能
 - TOPPERS新世代カーネル統合仕様書
- FTAにガイドワードを用いたもので実施
 - omission, commission, early, late
- 安全分析結果が導出し易いように論理ブロックを機能ごとに用意



[安全要求分析結果報告書.xls](#)

- 対策方法と安全要求事項
 - OSの決定論的原因故障に対する対策
 - IEC 61508 第1部の規定に従った開発プロセスを実施する。また、第3部の規定に従った設計・検証手法を用いる。
 - アプリケーションによるカーネルのサービスコールの誤使用に対する対策
 - OSコンポーネント取扱説明書を作成し、アプリケーションの誤使用を防止する。
 - ランダムHW故障に対するアプリケーションの支援機能
 - アプリケーションがランダムHW故障の対策を行うことを支援する故障検出ライブラリを提供する。
 - ランダムHW故障対策用 安全機能開発ガイドラインの作成
 - FSMPに従い安全機能開発ガイドラインを作成し、アプリケーションが対策を実施する際の注意点を記載する。
 - OSに求められるカーネル機能

- 分析対象: カートシステムのブレーキ機能
 - FlexRay電動カート システム要求仕様書
- 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
- FTAにガイドワードを用いたもので実施
 - omission, commission, early, late
- 安全分析結果が導出し易いように論理ブロックを機能ごとに用意



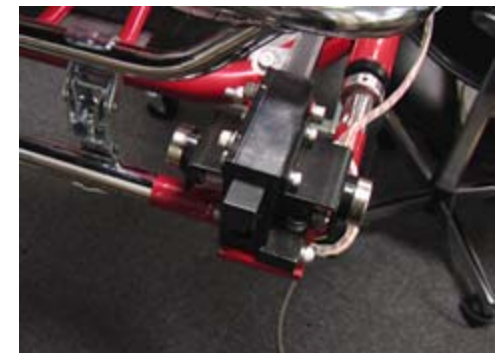
- 対策方法と安全要求事項

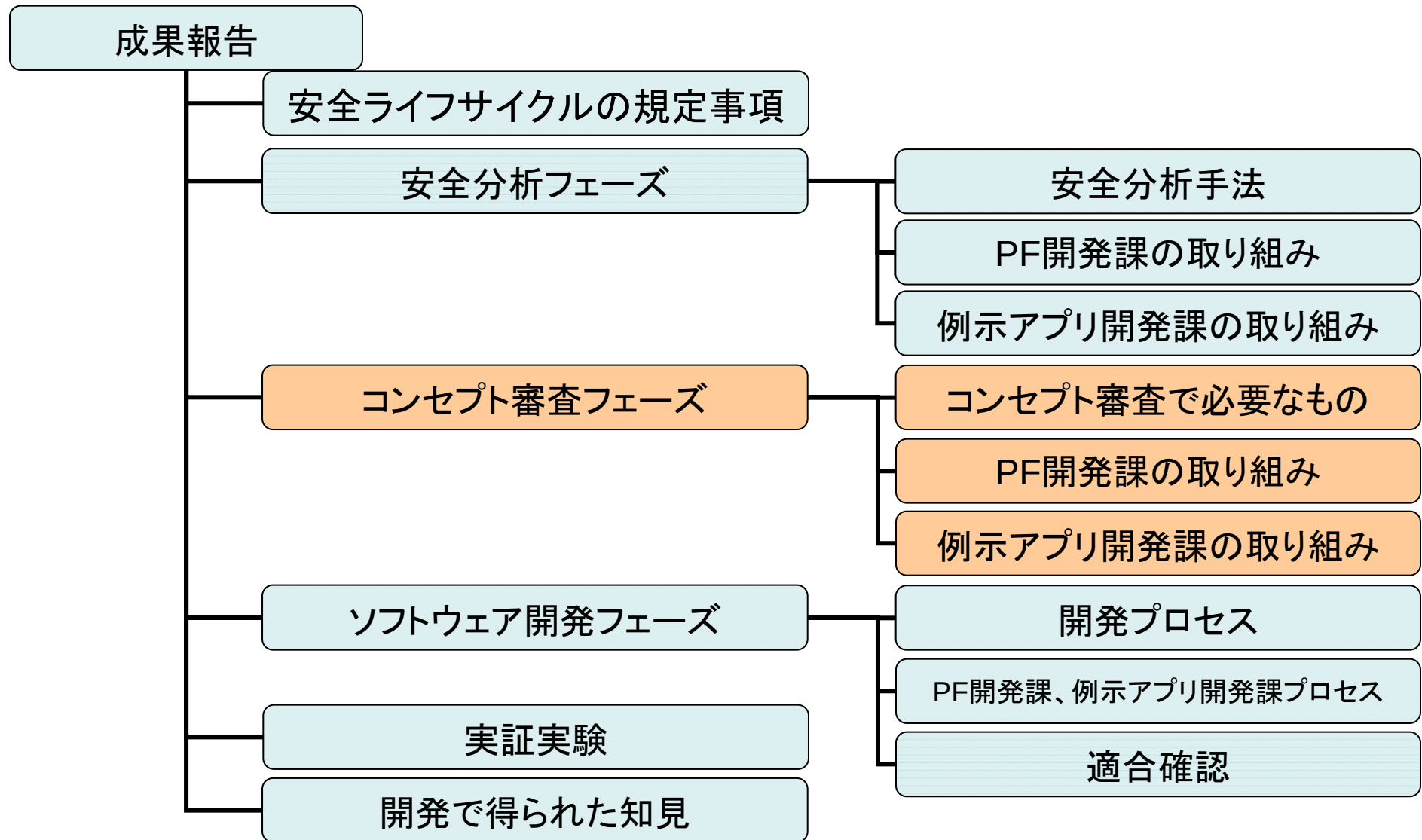
- 故障の対応(ソフトウェア)

- ブレーキセンサー値変換処理の異常、シーケンスの異常
 - ブレーキ稼動値の異常、FlexRay通信ミドルウェアの異常
 - 規定値の範囲確認、デッドラインモニタ、シーケンスモニタによる監視
 - 下記異常を検知して、オペレータ及び第三者へ視覚的・聴覚的に伝える。
またブレーキ機能を用いて自動停止制御を行う。

- 故障の対応(ハードウェア)

- ブレーキセンサーの破損、ブレーキセンサー値の固着
 - A/Dポートの破損、A/Dポートとコネクタ間のライン断線
 - ブレーキセンサーを二重系統にして且つソフトウェアにて監視する。
 - 手法からの導出
 - A6.5 入力比較、A.12.1 基準センサー、A.13.2 監視、
 - サーボモータの電源供給部にリミッターSWを据付ける





- 認証機関による開発フェーズに進むための審査
- 安全ライフサイクルの1～5の範囲が対象
 - 機能安全対応開発計画書(通称:FSMP)
 - IEC 61508によって規定される機能安全マネジメント(人、組織、技術)と開発計画を規定する
 - 安全コンセプト(通称:SC)
 - 安全分析を実施して導出された安全コンセプト
 - ソフトウェア安全要求仕様書(通称:SRS)
 - 対象システムにおけるE/E/PES安全要求事項を満たすために必要なソフトウェアの要求事項(ソフトウェア安全要求事項)を規定する。

- 開発対象：OSコンポーネント＜Safe OS＞
- 安全コンセプト
 - Safe OS = カーネル基本機能 + 故障検出ライブラリ
 - カーネル自体が安全関連系
 - アプリケーションによりハードウェアの故障検出を支援するライブラリ
 - Safe OS を用いたシステムに対して、故障検出率が90%～99%の診断機能を提供する
 - 開発プロセス：SIL3を満たす開発手法（IEC61508-3）

• ソフトウェア安全要求仕様書

– カーネル基本機能

- ITRON4.0仕様(TOPPERS/ASPカーネル) – 非安全関連利用機能

– 機能安全は対象範囲を必要最小限にすることが重要！

- » 安全に必要な機能に限定
- » 安全を担保しづらい機能を削除

– 故障検出ライブラリ

- ROMの故障検出チェック
- RAMの故障検出チェック
- 実行シーケンスモニタリング

安全機能
ガイドライン

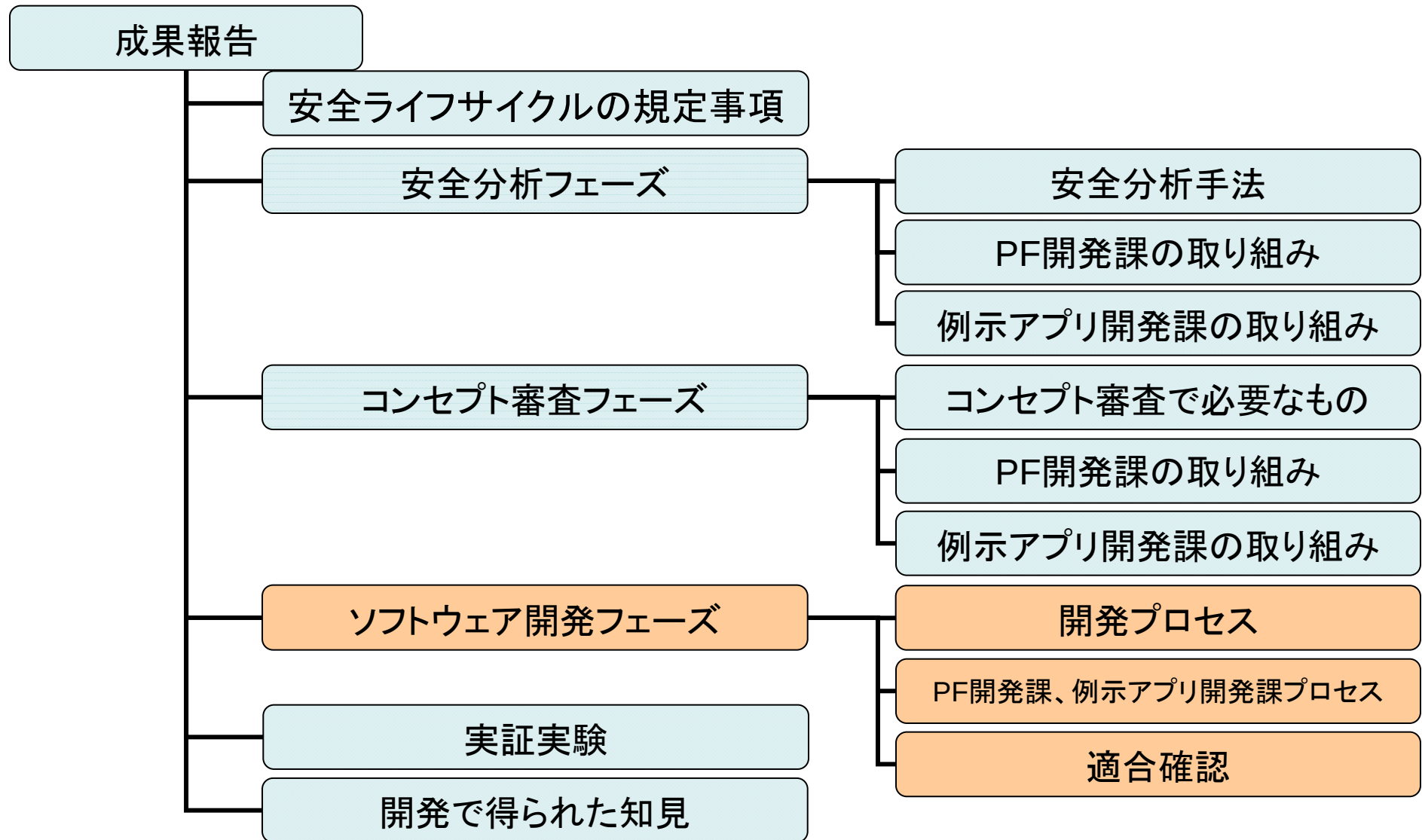


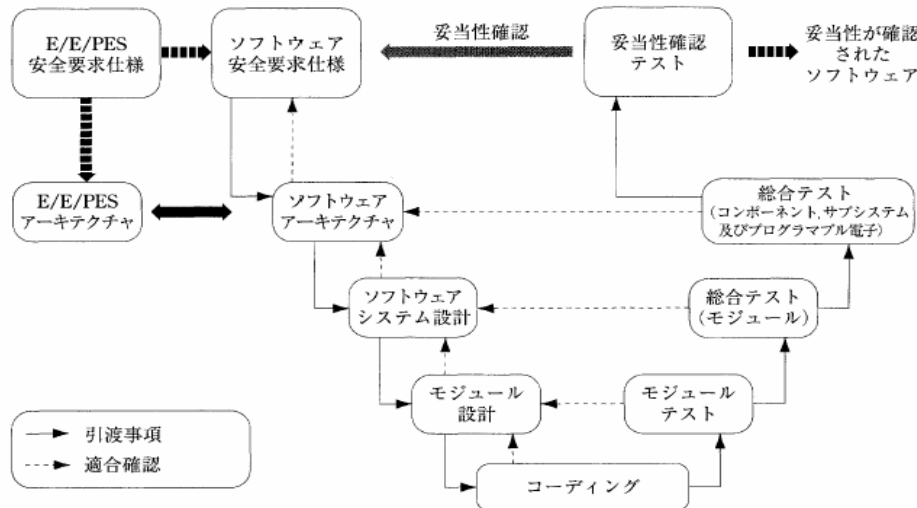
– Safe OSのユーザが対応（故障検出ライブラリでは対応しない）

- CPUの故障検出チェック # CPU依存のため
- 割込みコントローラの故障検出チェック # CPU依存のため
- バスの故障検出チェック # H/Wの対策が前提となり、S/Wだけでは対応不可

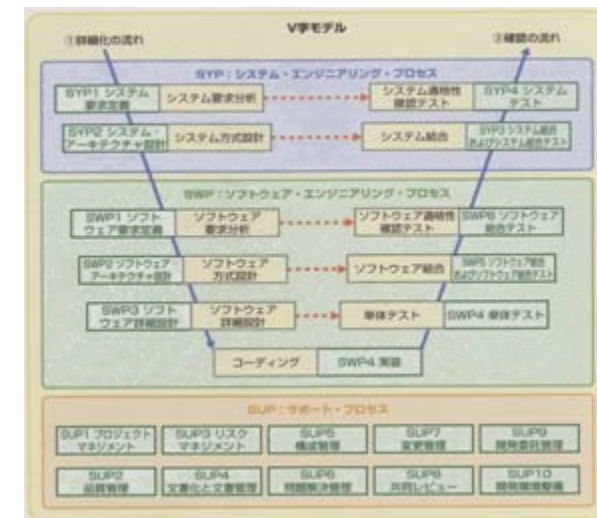
→ 「安全機能ガイドライン」としてユーザに情報を提供。

- 開発対象: FlexRay電動カート(ブレーキ機能)
- 安全コンセプト
 - 異常状態に陥ってもユーザの意図通りにカートを安全に止める
 - 開発プロセス: ブレーキシステムでSIL3を満たす開発手法(IEC61508-3)
- ソフトウェア安全要求仕様書(抜粋)
 - ブレーキ機能に異常が発生した場合、赤色LEDを点灯する。
 - ブレーキ機能に異常が発生した場合、ブザーを300ms間隔で鳴らす
 - センサーノードでの異常発生時は、自動停止制御を行う。
 - パワートレインノードでの異常発生時は、ユーザに通知を行い、自動停止制御を行う。
 - ブレーキセンサー値の2重チェックを行う。
 - ブレーキ処理の実行時間に対するソフトウェアデッドラインを検知する。
 - ブレーキ処理シーケンスにおける異常を検知する。
 - 自動停止制御は30ms以内に開始する。
 - 自動停止制御は6m以内で停止する。





JIS C 0508-1 より引用



ESPR Ver.1.0 より引用

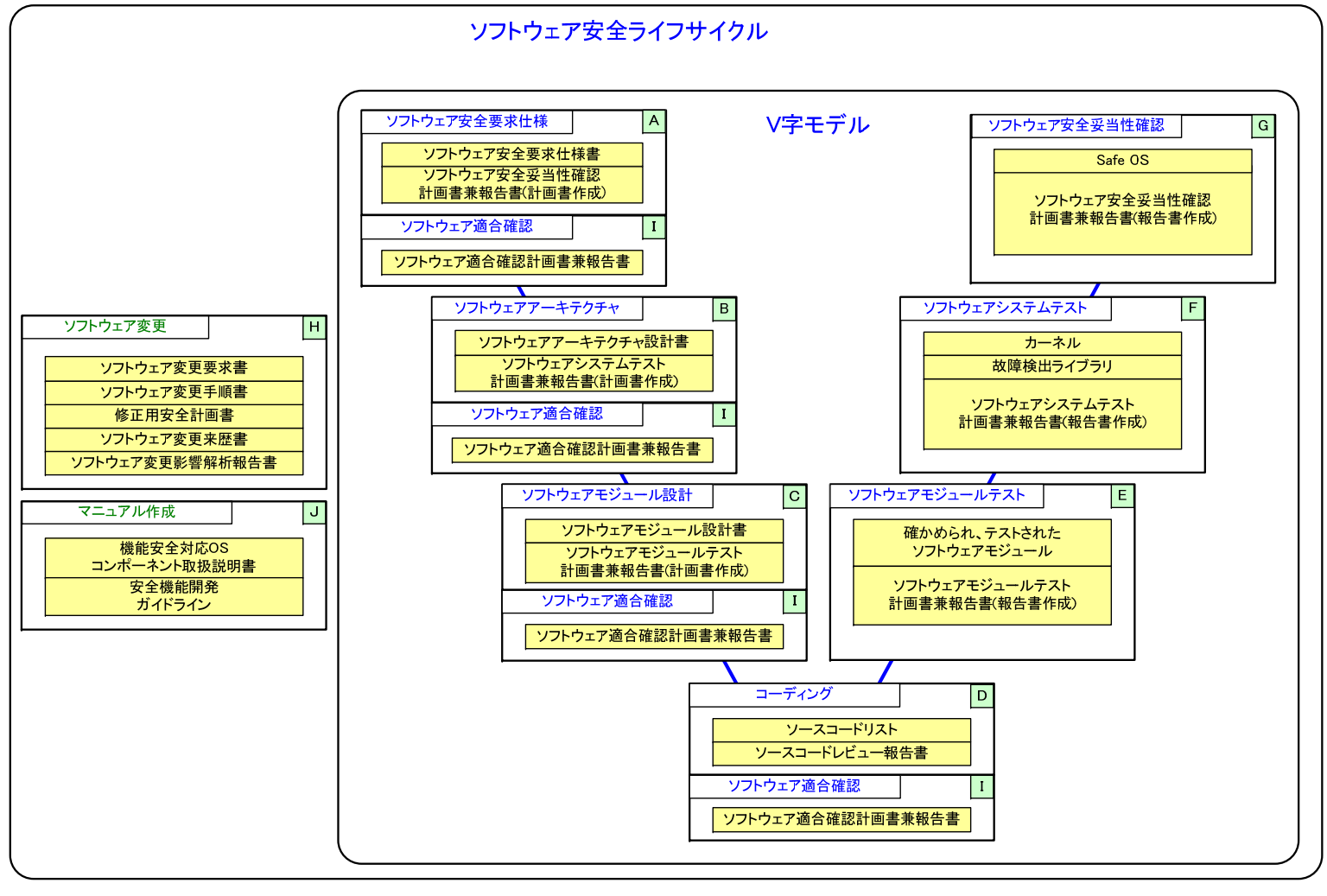
ソフトウェア開発で一般的に利用されているV字プロセスとほぼ同じプロセスが規定されているのでそのまま利用している。

IEC61508要求ドキュメント	本研究作成ドキュメント
(中略)	
SW安全計画書	ソフトウェア機能安全計画書
SW安全要求仕様書	ソフトウェア安全要求仕様書
SW安全アーキテクチャ設計説明書	ソフトウェア機能仕様書
コード化マニュアル	コーディング規約書
SWシステム設計仕様書	ソフトウェアコンポーネント設計仕様書
SWモジュール設計仕様書	ソフトウェアモジュール設計仕様書
SWモジュールソースコードリスト	ソースコードリスト

IEC61508はソフトウェア規格として各プロセスの入出力情報として文書を規定
 但し、要求するドキュメントはまったく同じ体系である必要は無く、開発で作成するドキュメントに含まれる内容と対比できれば良い

開発プロセス

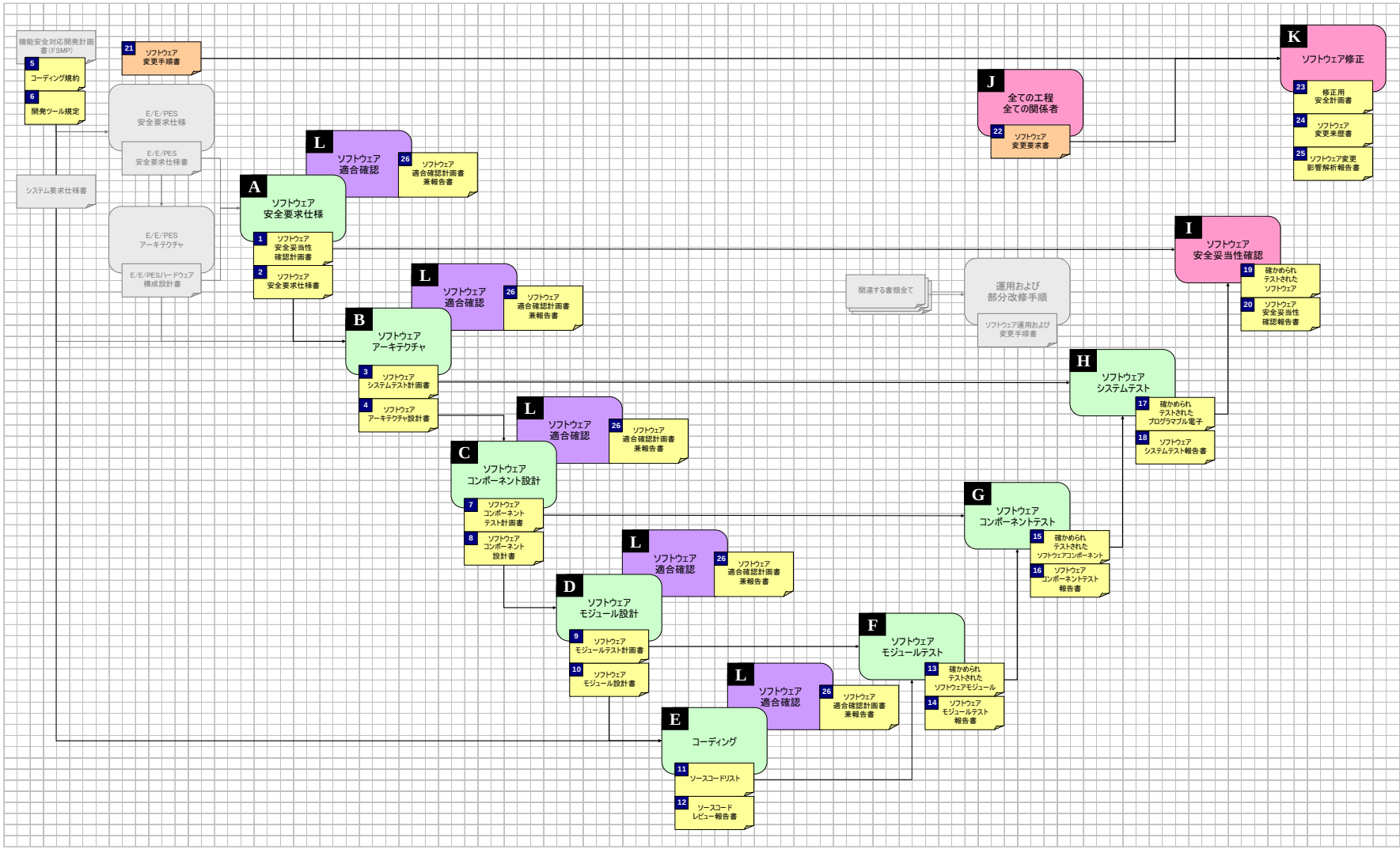
OSのV字モデルによる開発プロセスと成果文書



株式会社ヴィッツ

Embedded Technology 2009

開発プロセス



- ソフトウェア適合確認手順

- 各工程からの出力情報を試験及び評価し、その工程への規定に関する入力情報との正しさと整合性が取れていることを保障する。

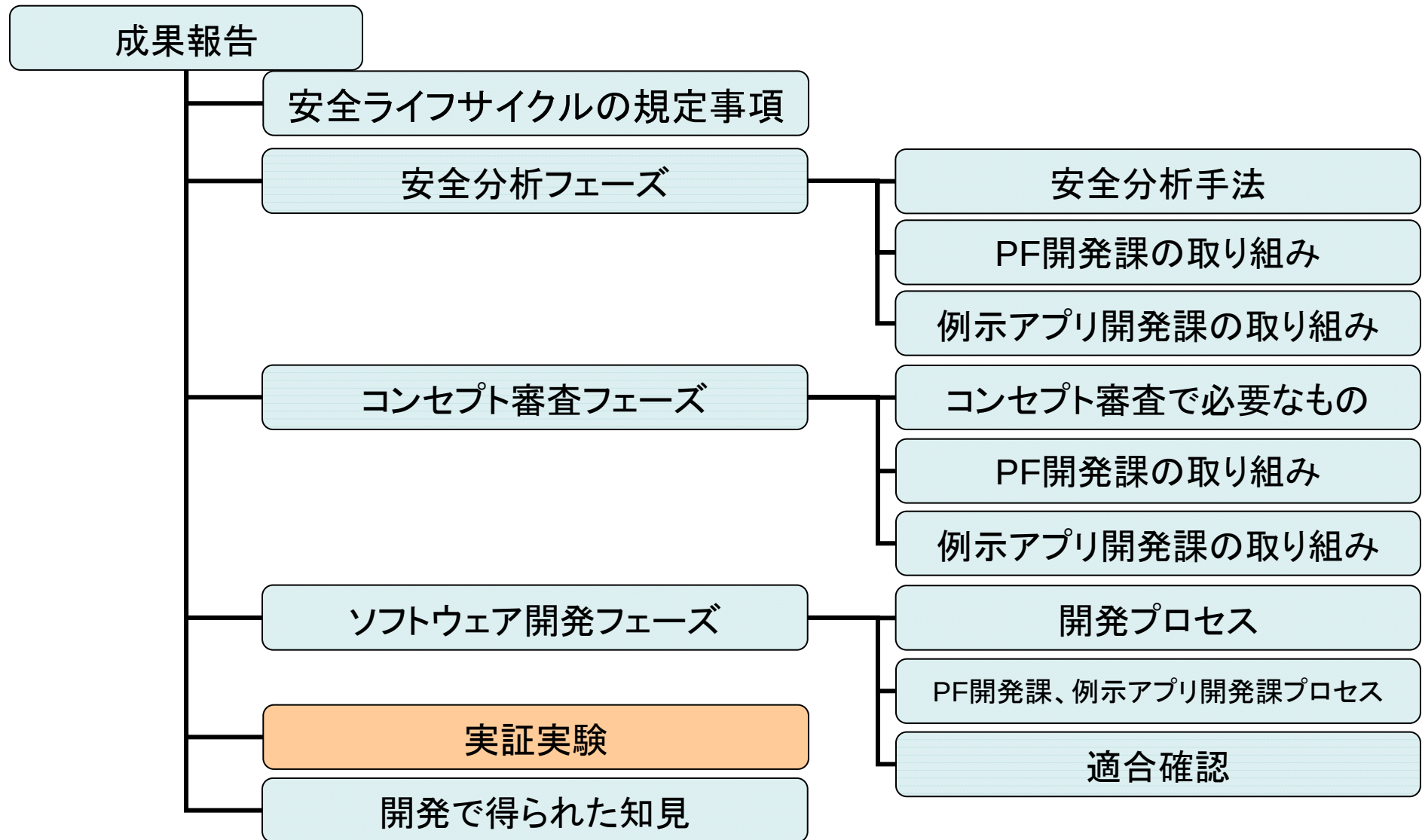
- 各工程実施時に「ソフトウェア適合確認計画書兼報告書」を作成

- 実施項目

- 要求仕様の整合性
 - トレーサビリティの確認
 - 手法の確認
 - ツールの確認
 - 必須事項の確認
 - テスト工程の実施結果の確認
 - ペンディング事項の評価

ソフトウェア適合確認計画書兼報告書 (ソフトウェア安全要求仕様).xls

株式会社ヴィッツ

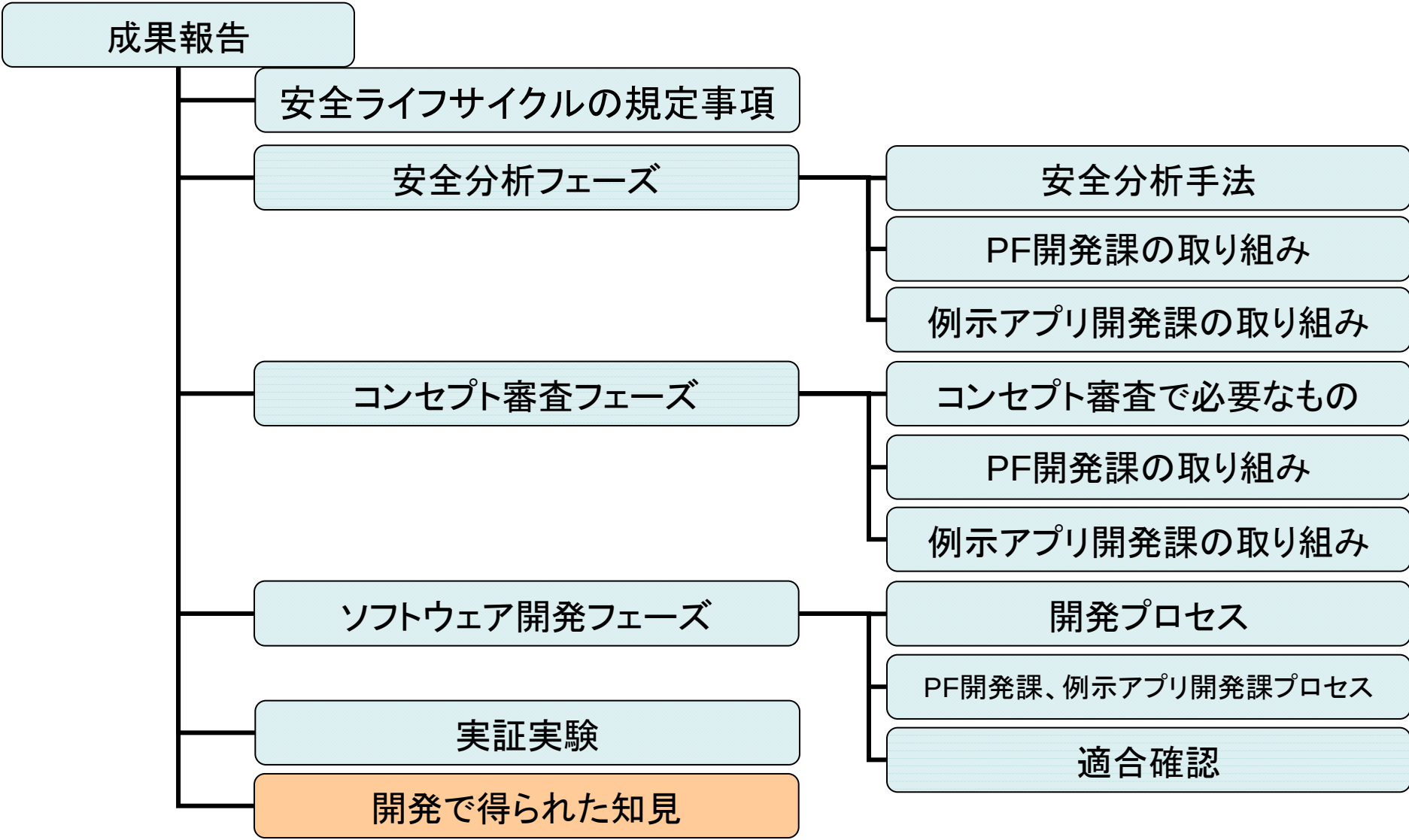


- 10月20日(火)
- 場所:トリトンサーキット
- 各開発課による実証実験を実施
 - 安全分析により抽出した安全要求事項を開発コンポーネントやアプリケーションに導入することで、搭載するFlexRay電動カートにて障害が発生しても安全性が保たれていることを確認する。



株式会社ヴィッツ





• 安全分析

– HAZOP手法を実施する前の決め事

• 影響、環境、ガイドワード、重要度

1	2	3	4	5	6	7	8	9	
1									
2		ソフトウェアHAZOPワークシート							
7	No.	アイテム	属性	ガイドワード	解釈	原因	ローカルな影響	グローバルな影響	
8	1				電圧がない	センサの異常により、電圧出力がない。 ブレーキペダルセンサとセンサノードの間の断線 ブレーキペダルセンサへの電源供給されない。	センサノードとバトロード間のデータが常に0である。→サーボモータへのブレーキ量が初期値のままである。	ブレーキがきかない	
9	2								
10	3								
11	4								
12	5								
13	6								
14	7			no	0ボルト	回路の設計によっては回路の断線 GND線とショート センサが故障 ブレーキペダルセンサへの入力が0(人間は踏んだつもりが踏んでない) ブレーキペダルセンサへの入力が0(人間はブレーキ踏んだ) ブレーキペダルセンサより前が故障	サーボモータが動かない	止まらない	マイコンが0ボルトを接 ブレーキ非 カートの前 断線し難い 配線を二重
15	8								
16	9								
17	10				電圧が想定より低い	センサの異常により、電圧出力が低い。 ブレーキペダルとセンサの間のメカ的な故障 センサへの電圧供給が低い センサが故障	センサノードとバトロード間のデータが正常値より小さい。→サーボモータへのブレーキ量が正常値より小さい。	ブレーキの利きが悪い	
18	11								
19	12								
20	13								
21	14								
22	15								
23	16								
24	17								
25	18			less	想定値より小さい (規定値の定義が無い場合、公差範囲)	センサの稼働範囲の規定値がずれている あまり踏んで無いつもりが踏んでいた ペダルの調整不備	サーボモータの移動量が少ない	ブレーキのききが悪い 制動距離が長くなる	規定値を規定値外の規定値より増幅回路に異常に近い ドライバへ

• ソフトウェア開発

– 開発プロセスや手法を意識した開発

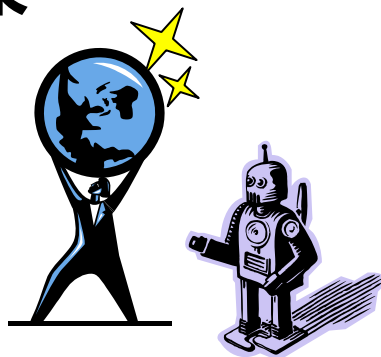
機能安全ソリューションの紹介

ヱッツ機能安全ソリューション

機能安全規格適応効果

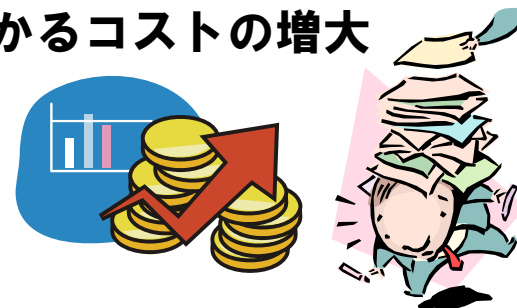
■ メリット

- ・ 信頼性/安全性の向上
- ・ 企業ブランド力の向上
- ・ 国際競争力の向上



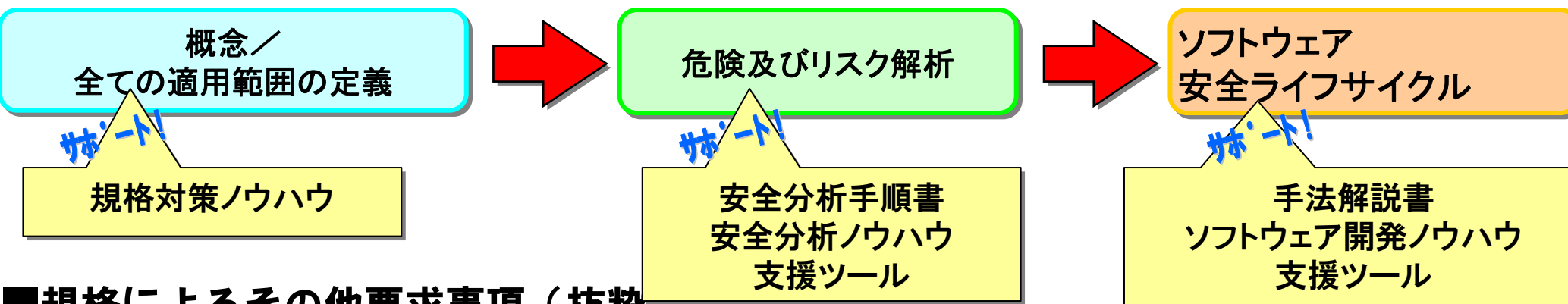
■ 企業側の負担

- ・ 機能安全対応に掛かるコストの増大
- ・ 開発規模の増大

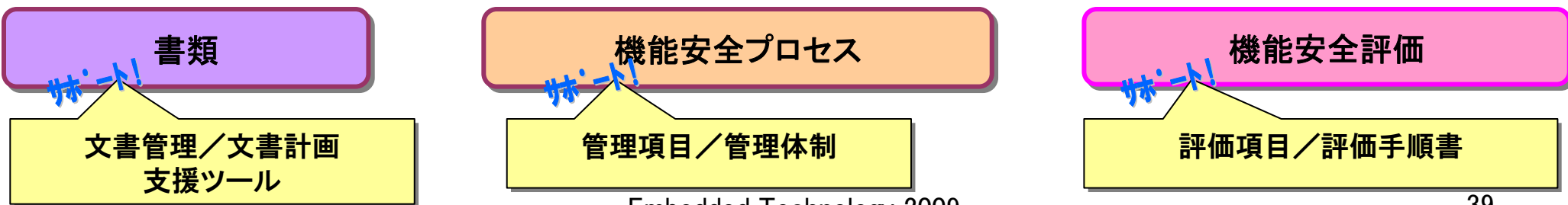


機能安全規格適応の流れ

■ 規格による技術要求事項（抜粋）



■ 規格によるその他要求事項（抜粋）



- 機能安全開発支援ツール

- 平成21年度 全国中小企業団体中央会 試作開発等支援事業
- 目的: 機能安全開発を支援するツールの開発

安全設計支援ツール	システム構成をブロック図で表現し、故障率、通信エラーレート、自己診断率等の情報を元に、システムの故障率(SIL)を算出する。
安全分析(HAZOP) 支援ツール	システム構成情報を元に、HAZOPワークシートの雛形を生成する。
FSMP作成支援ツール	FSMPに必要な情報を入力し、コンセプト審査を通るレベルのFSMPの雛形を生成する。
トレーサビリティ管理支援ツール	要求/設計/テスト項目レベルのトレーサビリティ管理を支援するツール。各項目の関連表の生成、変更時の影響分析も行える。

※機能安全開発支援ツールのプロトタイプモデルがヴィッツブースに展示して有ります。

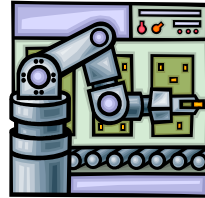
サポート実績紹介（一部）

■A社

産業機器の新規開発サポート

<サポート内容>

- ・プロジェクト立ち上げ
- ・設計／開発
- ・管理



■B社

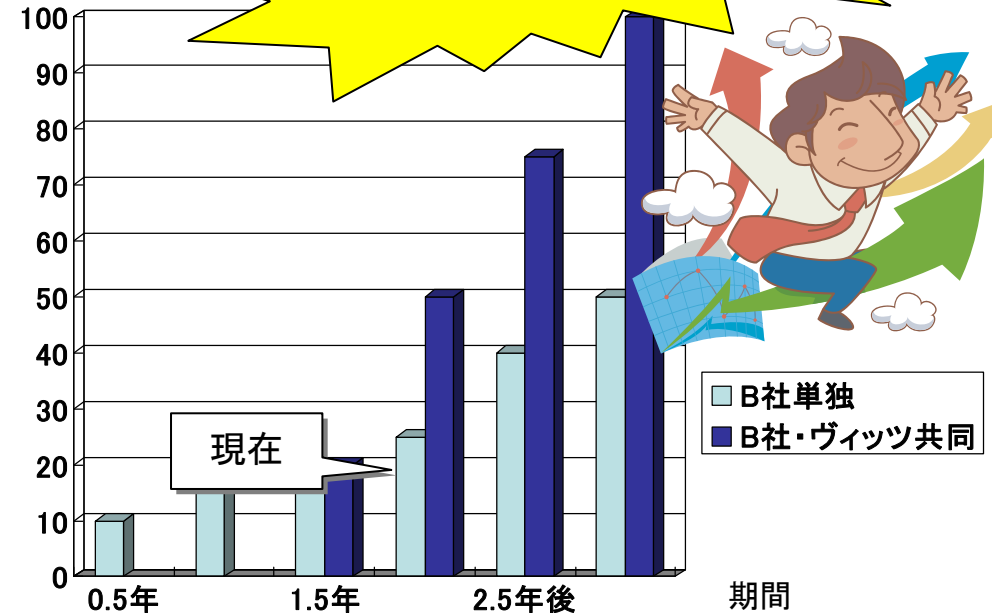
産業機器の開発サポート

<サポート内容>

- ・設計／開発



進捗率



**ヴィッツでは豊富な開発経験を生かし
機能安全規格適応までを強力サポート致します！**



ご清聴ありがとうございました。