本スライドは、当日のセミナー資料から一部を抜粋したものです。

ISO26262における ソフトウェア開発プロセス

株式会社ヴィッツ
組込制御開発部 機能安全開発室
室長　森川 聡久

機能安全の達成に必要なこと（安全証明）

機能安全 ＝ 安全証明

・第3者（認証機関、ユーザら）によって、**安全であることを確認できる必要**がある。
・大きくは、安全プロセス・安全設計の2つの側面から。

①「機能安全管理規定」が機能安全規格を満たしていること。
②実際の開発が、「機能安全管理規定」に定めた通りに行われていること。
⇒「機能安全管理規定」が肝。

③システムの「安全コンセプト」が機能安全レベルを満たしていること。
（安全目標、安全分析、安全要求仕様、安全設計、安全マニュアル等）
④開発途中の成果物が全て問題のないこと。
（トレーサビリティ、独立検証）
⑤最終成果物が当初の「安全コンセプト」を満たしていること。
（機能試験、環境試験、故障挿入試験等）
⑥最終システムの故障率が、SILを達成していること。
⇒「安全コンセプト」が肝。

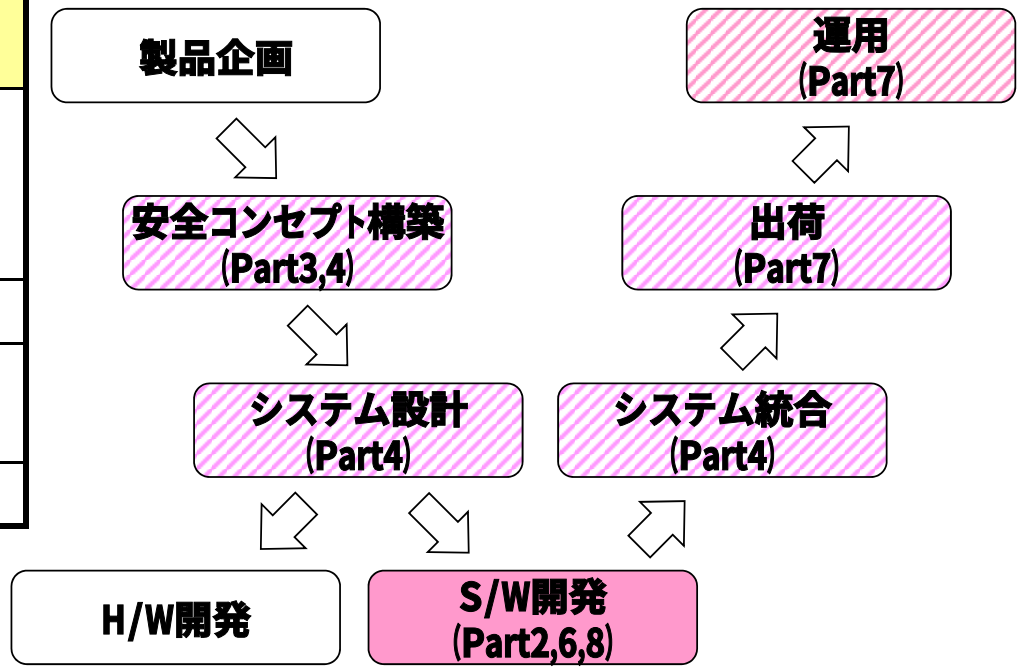
コンセプトフェーズ
①③

実現フェーズ
V
⑤⑥
②④

ソフトウェア開発に関する要求範囲

ISO 26262	要求事項
Part2	機能安全開発プロセス（開発、管理）
Part6	
Part8	
Part3	ソフトウェアにおける安全策
Part4	ソフトウェアにおける安全策 システム開発との連結方法
Part7	ユーザへの要求事項

機能安全開発の全体の流れ



＜Part2＞
5 全体的な安全な管理
6 コンセプトフェーズと製品開発間のプロジェクト管理
7 製品リリース後の安全管理

＜Part6＞
5 ソフトウェアレベルにおける製品開発の開始
6 ソフトウェア安全要求の詳細仕様
7 ソフトウェアアーキテクチャ設計
8 ソフトウェア単体の設計および実装
9 ソフトウェア単体テスト
10 ソフトウェア結合およびテスト
11 ソフトウェア安全要求妥当性検証
Annex C ソフトウェアコンフィグレーション

＜Part8＞
5 分担開発内のインターフェース
6 安全要求の仕様と管理
7 コンフィグレーション管理
8 変更管理
9 ベリフィケーション
10 文書化
11 ソフトウェアツールの検定
12 ソフトウェアコンポーネントの検定
13 ハードウェアコンポーネントの検定
14 使用過程証明済の立証

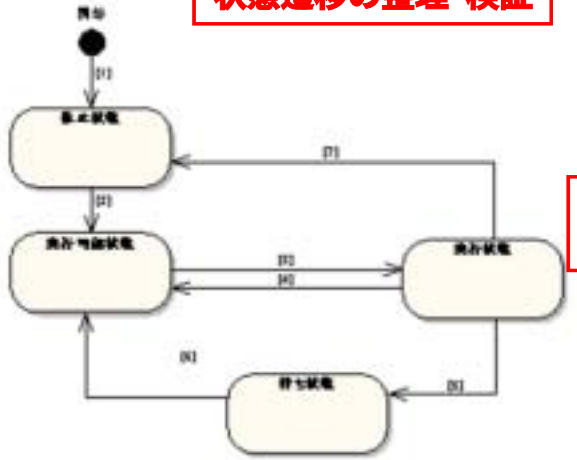
これらを FSMP (Functional Safety Management Plan ；機能安全管理計画) 規程文書としてまとめる。
基本的に FSMP は開発製品毎に準備する。
ISO9000のQM (Quality Management) や Automotive-SPICEの管理規定と極端な差はない

準形式手法の実施例

※当社RTOS開発文書より抜粋

状態遷移図

状態遷移の整理・検証



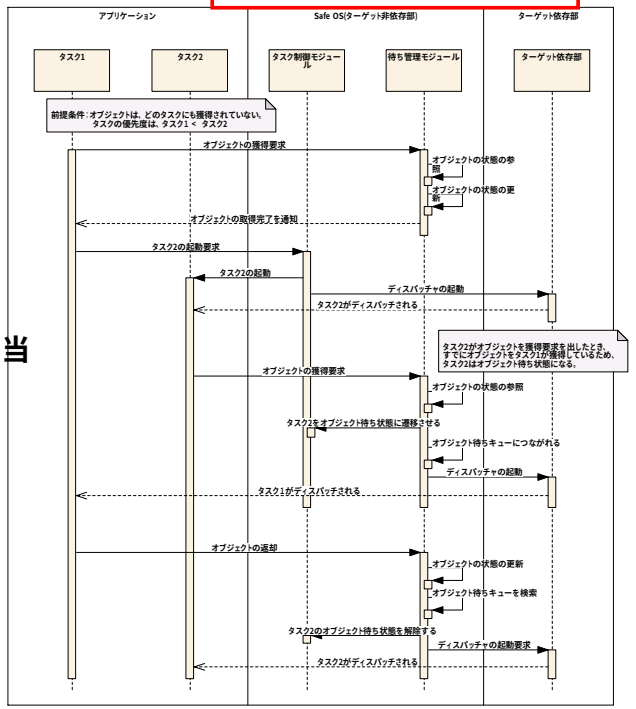
＋

状態・時間の組み合わせ検証

＝タイムペトリネット相当

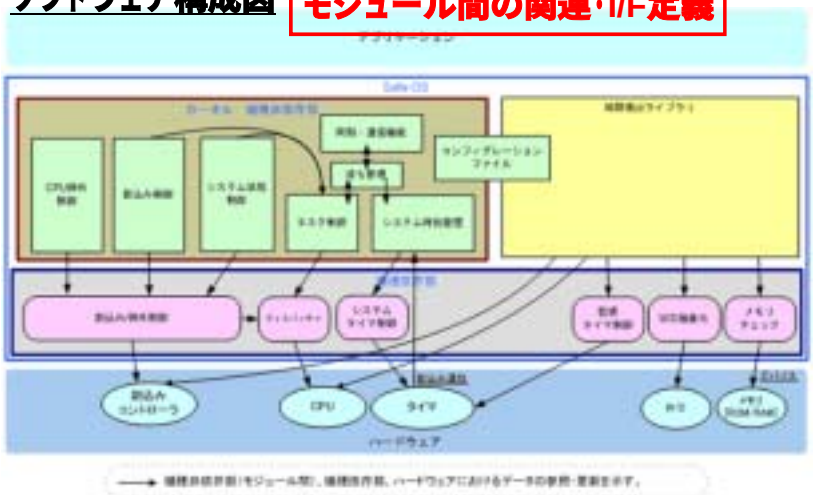
シーケンス図

シーケンスの整理・検証



ソフトウェア構成図

モジュール間の関連・I/F定義



決定表

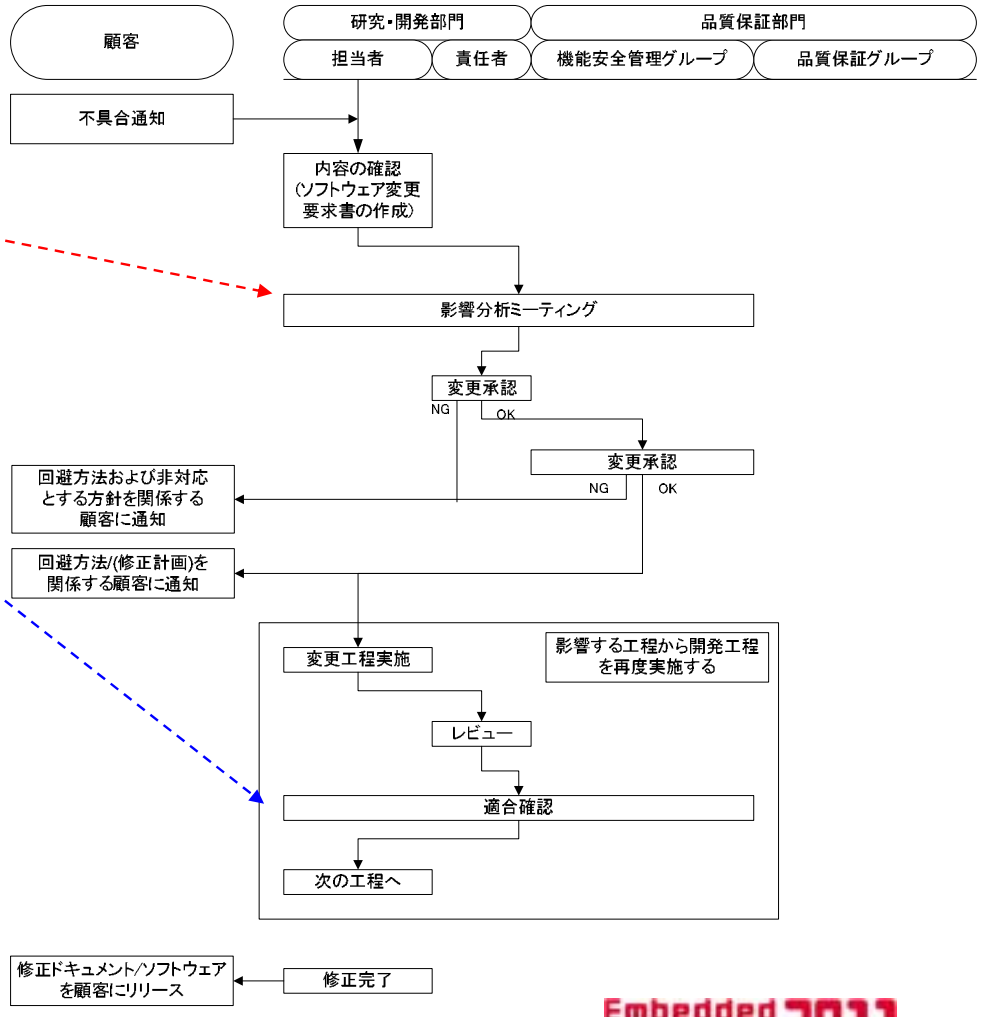
複雑な条件実行の整理・検証

カーネルへの処理要求	割込みハンドラ	Y	N	N	N
	タスクで発生したCPU例外ハンドラ	-	Y	N	N
	タスク処理要求　優先度 現在のタスクより高い	-	-	Y	N
	タスク処理要求　優先度 現在のタスク以下	-	-	-	Y
ディスパッチャ	ディスパッチ処理が実行される	-	-	X	-
実行される処理単位	割込みハンドラ	X	-	-	-
	CPU 例外ハンドラ	-	X	-	-
	タスク処理　優先度 現在のタスクより高い	-	-	X	-
	タスク処理　優先度 現在のタスク以下	-	-	-	X

ソフトウェア変更プロセス

- 完成されたソフトウェアを変更する場合は、慎重に対応する必要がある。
- 影響分析
  ＋
  再検証（Verification）
  が必須。
- 変更管理、構成管理、組織間の連携とも深く関連する。

例）当社の機能安全認証プロセスより抜粋



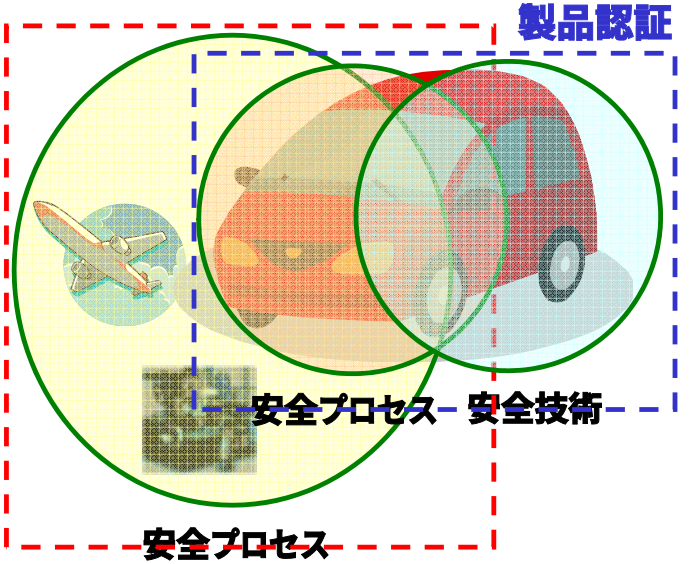
TUVの機能安全認証の種類

機能安全では、製品毎に認証を行う。(製品認証)

一方、認証機関 (TÜV) は、以下の2種類の認証形態を提供している。

	プロセス認証	製品認証
概念	「規定 (安全プロセス)」に対する認証	「結果 (安全プロセス＋安全設計)」に対する認証
適用範囲	さまざまな製品に適用可能	製品毎に認証が必要
有効期限	3年間	製品が破棄されるまで
開発プロセス	汎用的な開発プロセス	製品に特化した開発プロセス
対象ハードウェア	限定できない	固定

製品に特化



プロセス認証

複数の製品は勿論、
広範囲の産業に共通に適用可能

＜注意事項＞
- **認証取得有無によらず、開発時に実施する内容は同じ。**
  (誰が実施するかの違い。認証機関コストの差程度)
- **ソフトウェアプロセスは、どの機能安全規格でもほぼ同等。**