車載用機能安全規格ISO26262に対応した高信頼開発プロセスと活動

2012年10月11日

パナソニック(株)デバイス社
開発本部　機能安全・DR推進グループ
安倍秀二

機能安全規格とは

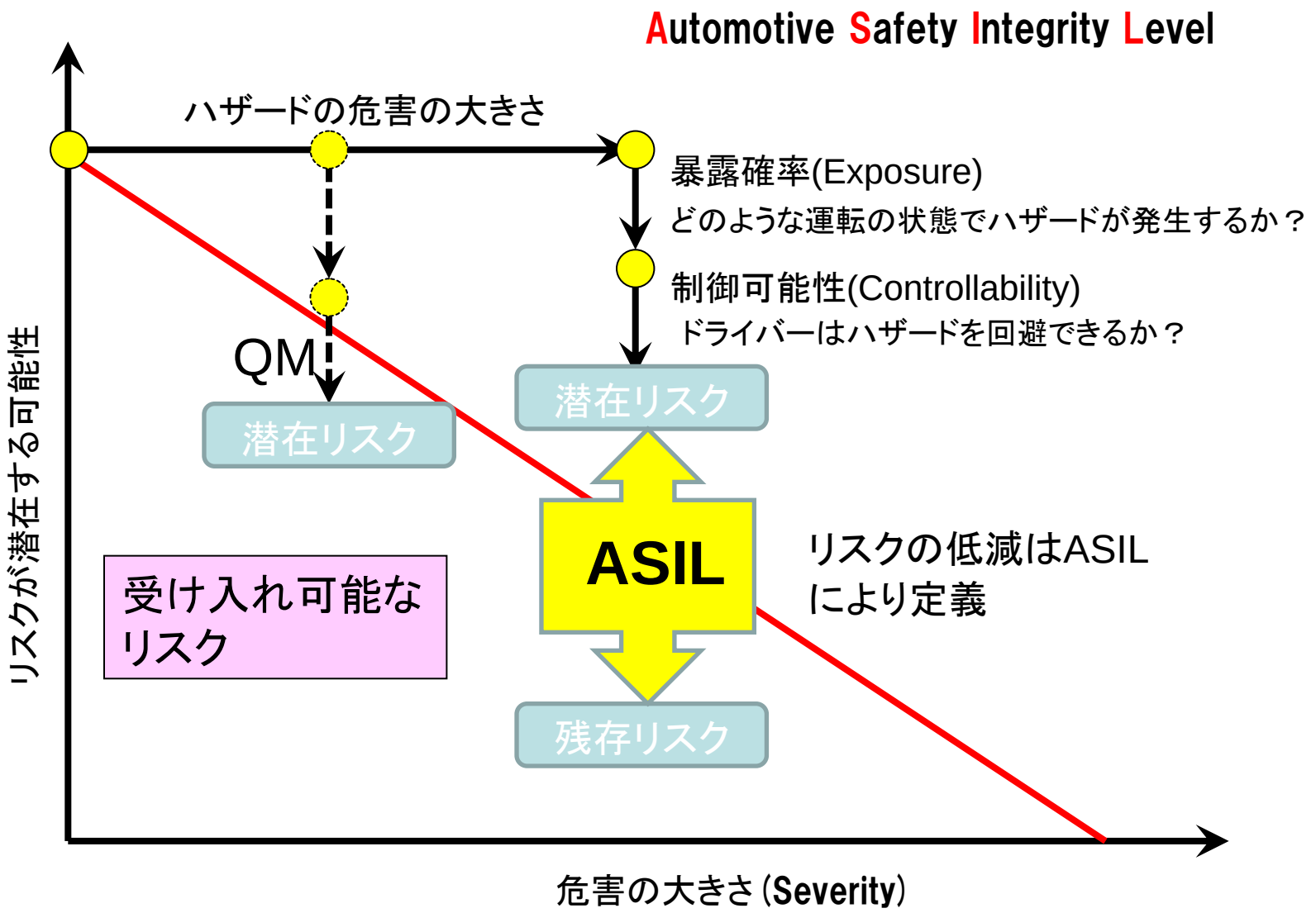
Panasonic
ideas for life

- 開発したシステムが安全であることを客観的に第三者に説明できること
- 訴訟への備え
- 車両システムが持つ不安全のリスクをASILの4段階で表示。不安全のリスクを顕在化させないための要求を定義。

※ASIL: Automotive Safety Integrity Level

ASILの概念

Panasonic
ideas for life



機能安全規格が求めること

Panasonic
ideas for life

- 安全ライフサイクル
- 詳細なプロセス定義
- コンファメーション方策
- 安全ケース
- 詳細な手法、技法
- ハードウェア部品の故障の定量評価
- ソフトウェアツールの適格性確認
- コンポーネントの適格性確認

曖昧な定義も多い

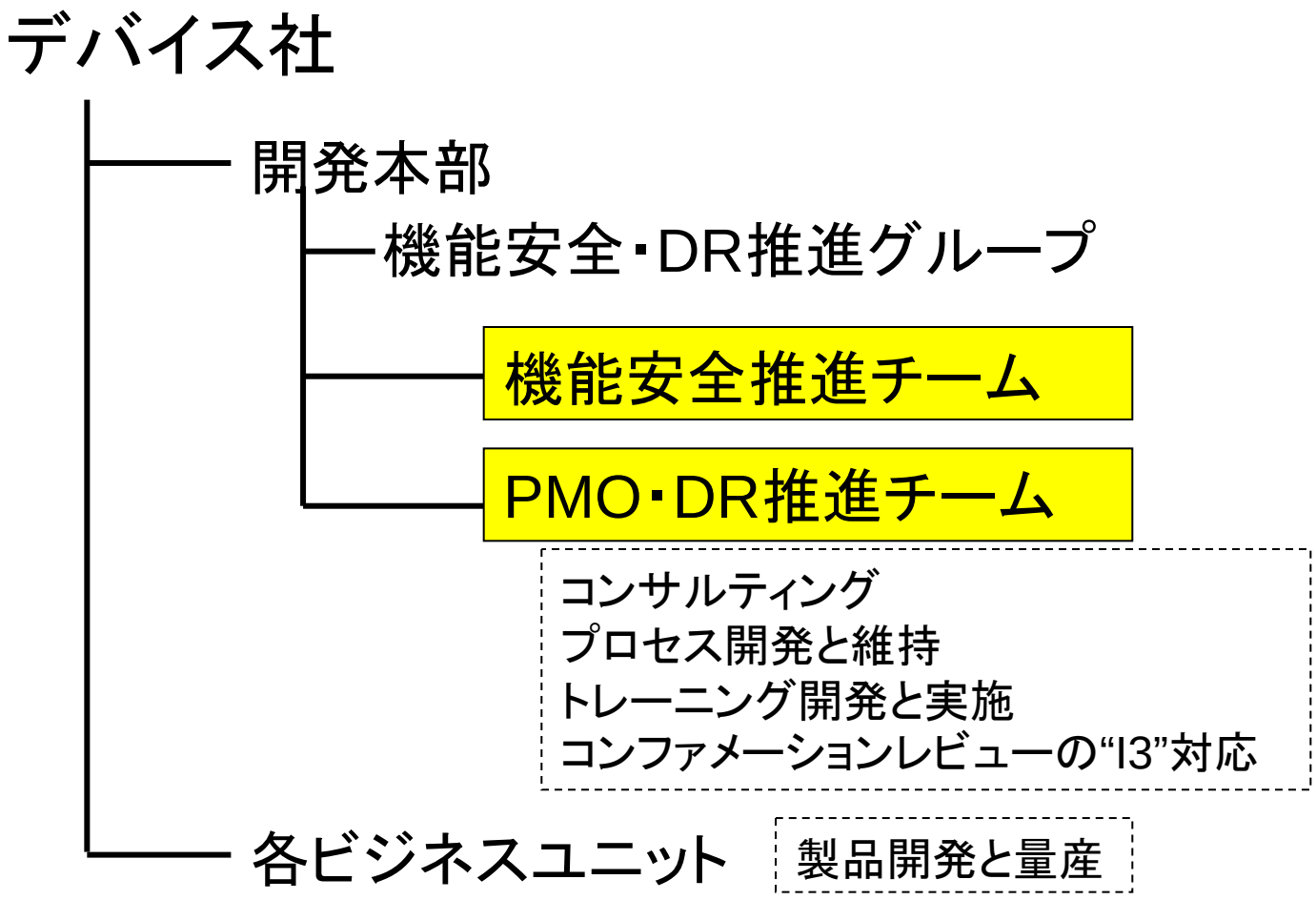
プロセスへ求められるもの

Panasonic
ideas for life

- 規格のもつ抽象性と具体性、曖昧性をどう扱うか？
- 顧客要求のプロセスの内装
  - AutomotiveSPICEとCMMI
- 非車載、ASIL非適用の開発も考慮
- 既存のプロセスをどう活かすか
- 従来の製品開発のフローを変えない
- 従来の成果物体系を大きく変えない

デバイス社における機能安全推進体制

Panasonic ideas for life



規格のインパクトを予感→専門組織

機能安全プロセス開発

Panasonic
ideas for life

- プロセス認証活動
  - パナソニック全社横断により、機能安全プロセスを開発
  - ベースのプロセスはデバイス社のものを提供（システム製品開発管理規程、システム/ハードウェア/ソフトウェア開発基準、テンプレート、チェックリスト）
  - 機能安全規格の翻訳、要求事項の分析
  - 機能安全ガイドラインに落とし込み
- 活動機関
  - 2011/4～2012/3
  - 2012/2/29　認証取得

社内メンバーを巻き込んだ共通理解

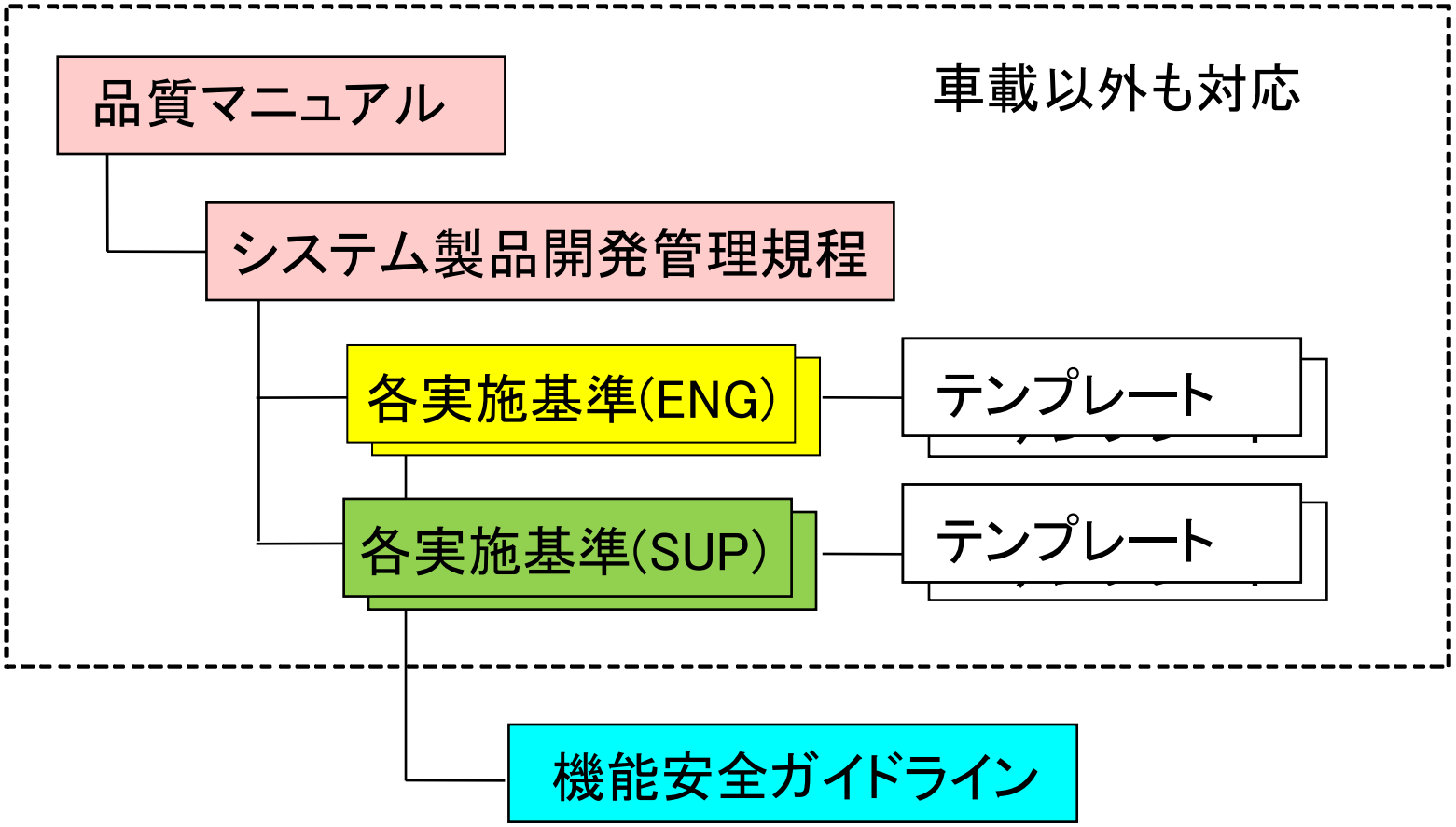
留意したこと

Panasonic ideas for life

- 安全ライフサイクル
  - 過去から構築してきたAutomotiveSPICE/CMMI対応のソフトウェアプロセスをベースに拡張
  - ASIL車載、ASIL非適用車載、非車載に対応
  - 機能安全規格専用のしくみをつくらない
  - ハードウェア開発をいかに巻き込むか
- 安全を確認するコンファメーション方策の導入
  - 新たに導入せずに、これまでに実施している組織活動に割り当てる。
    - コンファメーションレビュー、機能安全監査、機能安全アセスメント
  - ISO26262特有の内容は補足する（独立性、レビュー技法など）
- 手法の導入
  - SWはこれまでの活動に比較して追加項目は少ない
- 安全コンセプト形成とそのための分析が最重要
- ハードウェアの評価指標
  - 故障率などは確認していたが、定量的な評価指標はあらたな活動が必要。

開発リソースは限られている。新たな仕組みにしない

4層のプロセス構造

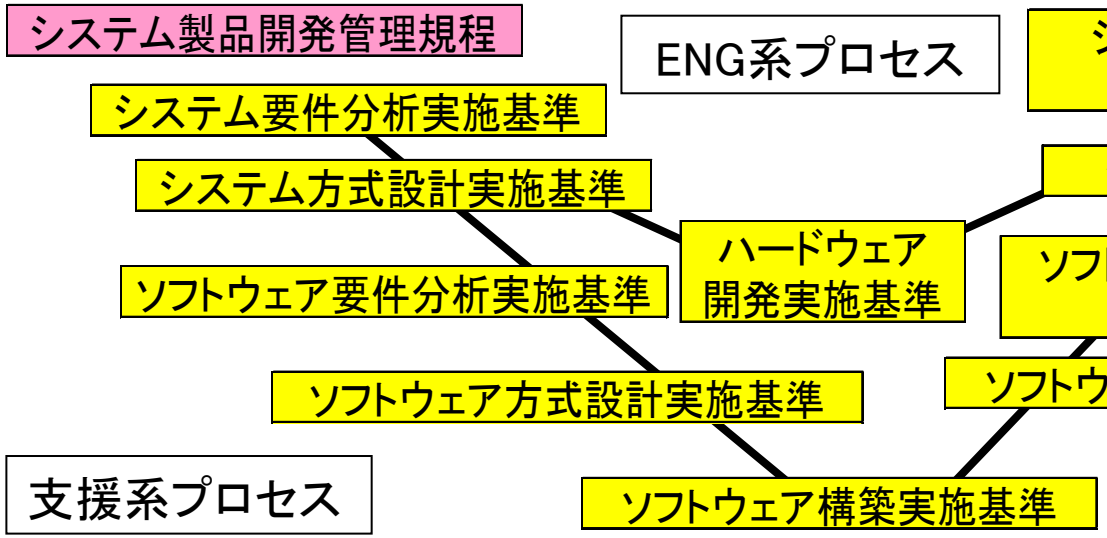


※組織関連のプロセス（改善、測定など）は各組織で準備

開発は機能安全/車載だけではない

プロセス構成

Panasonic
ideas for life



※プロセス構成のベースはAutomotiveSPICE CMMIの要素も含む

支援系プロセス

- プロジェクト計画策定基準
- プロジェクト管理基準
- 要件管理基準
- 構成管理基準
- 問題解決実施基準
- システム製品変更管理基準
- 外注管理基準
- システム製品DR実施基準
- システム製品品質監査実施基準
- システム製品AQチェック及び製品審査実施基準

機能安全ガイドライン

- 安全要件定義ガイドライン
- システム設計ガイドライン
- システムテストガイドライン
- ソフトウェア設計ガイドライン
- ソフトウェアコーディングガイドライン
- ソフトウェアコード分析ガイドライン
- ソフトウェアテストガイドライン

- MBD開発ガイドライン
- 安全分析ガイドライン
- 機能安全計画策定ガイドライン
- スキル認定ガイドライン
- ソフトウェアツール認定ガイドライン
- ソフトウェアコンポーネント認定ガイドライン
- ハードウェア設計ガイドライン

従来のプロセスを活かす

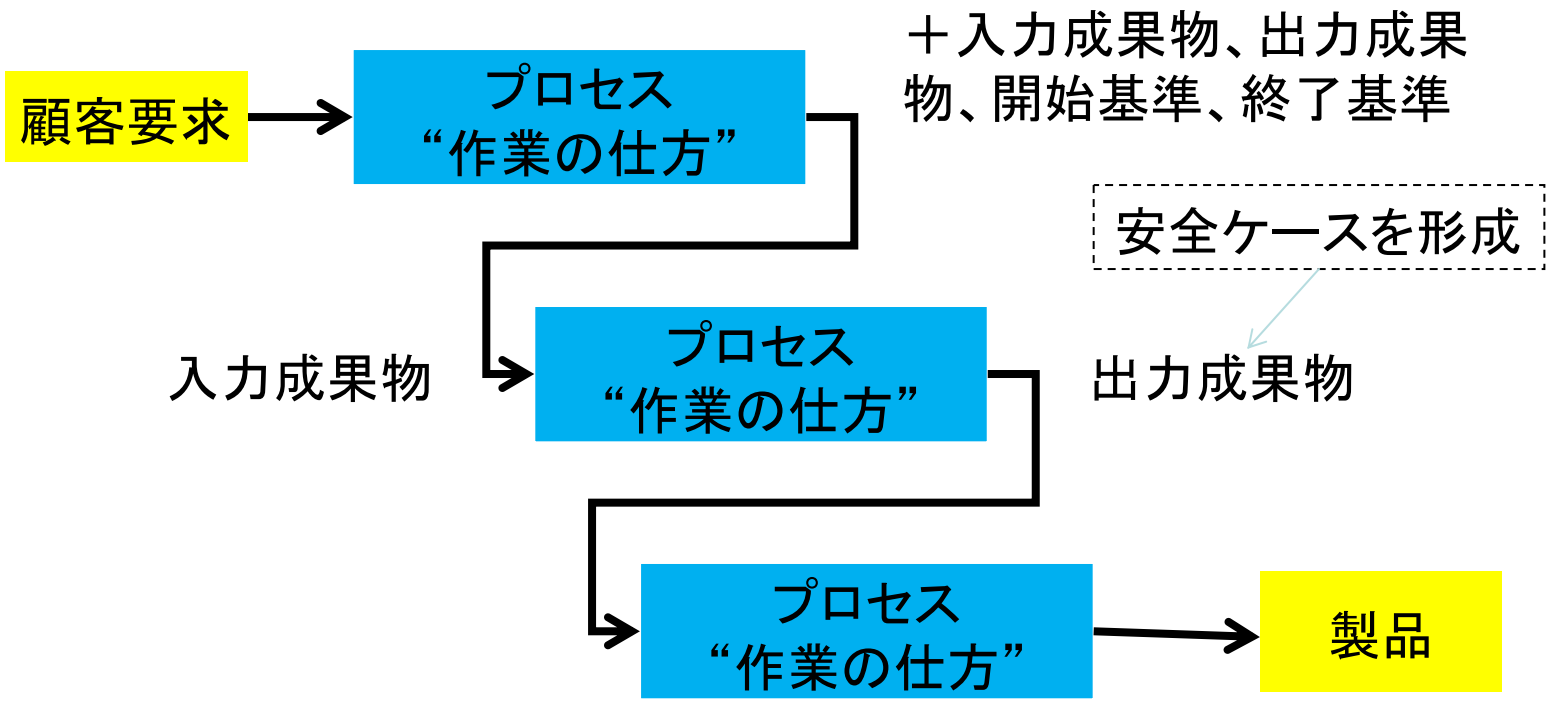
プロセスの特徴

Panasonic
ideas for life

- 従来からのソフトウェア開発プロセスにハードウェア部分を強化
  - CMMIとAutomotiveSPICEの内装
- 開発プロセスと機能安全要求を分離
  - プロセスの活動から関連する機能安全活動を記載した機能安全ガイドラインを呼び出す
- 制度化の部分で安全文化を形成
  - マネジメントとコンファメーション方策により確実なプロセス遵守

ASIL適用/非適用、車載・非車載に対応

プロセスアプローチ



- プロジェクトは、プロセスを利用して、各プロセスの出力をつないで入力成果物（顧客要求）から出力成果物（製品）を生み出す
- 実際のプロセスのつながりは、プロジェクト計画（反復計画）で詳細化。

トレーサビリティの確立

安全ケース

Panasonic
ideas for life

安全目標
機能要求

機能安全
コンセプト

増えた

仕様化

技術安全
コンセプト

システム
要件仕様書

システム
アーキテク
チャ設計書

ソフトウェア
要件仕様書

ハードウェア
要件仕様書

ソフトウェア
アーキテク
チャ設計書

ハードウェア設計書

ハードウェアメトリッ
ク

ソフトウェア
詳細設計書

回路図

P板パターン

ソースコード

部品明細

各プロセスの出力成果物で構成

＋レビュー記録
＋コンファメーション方策結果

各テスト計画と結果

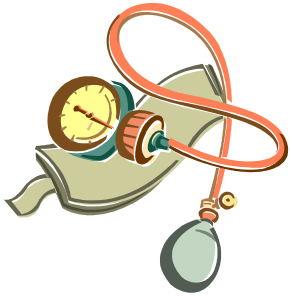
- システム適格性確認テスト
- システム結合テスト
- ソフトウェア適格性確認テスト
- ソフトウェア結合テスト
- ハードウェア結合テスト
- ユニットテスト
- ハードウェア機能ブロックテス

プロセス出力成果物で構成

コンファメーション方策の活動

コンファメーションレビュー

ISO26262の要求が
正しく実装されているか



機能安全アセスメント

製品は安全か？

機能安全監査

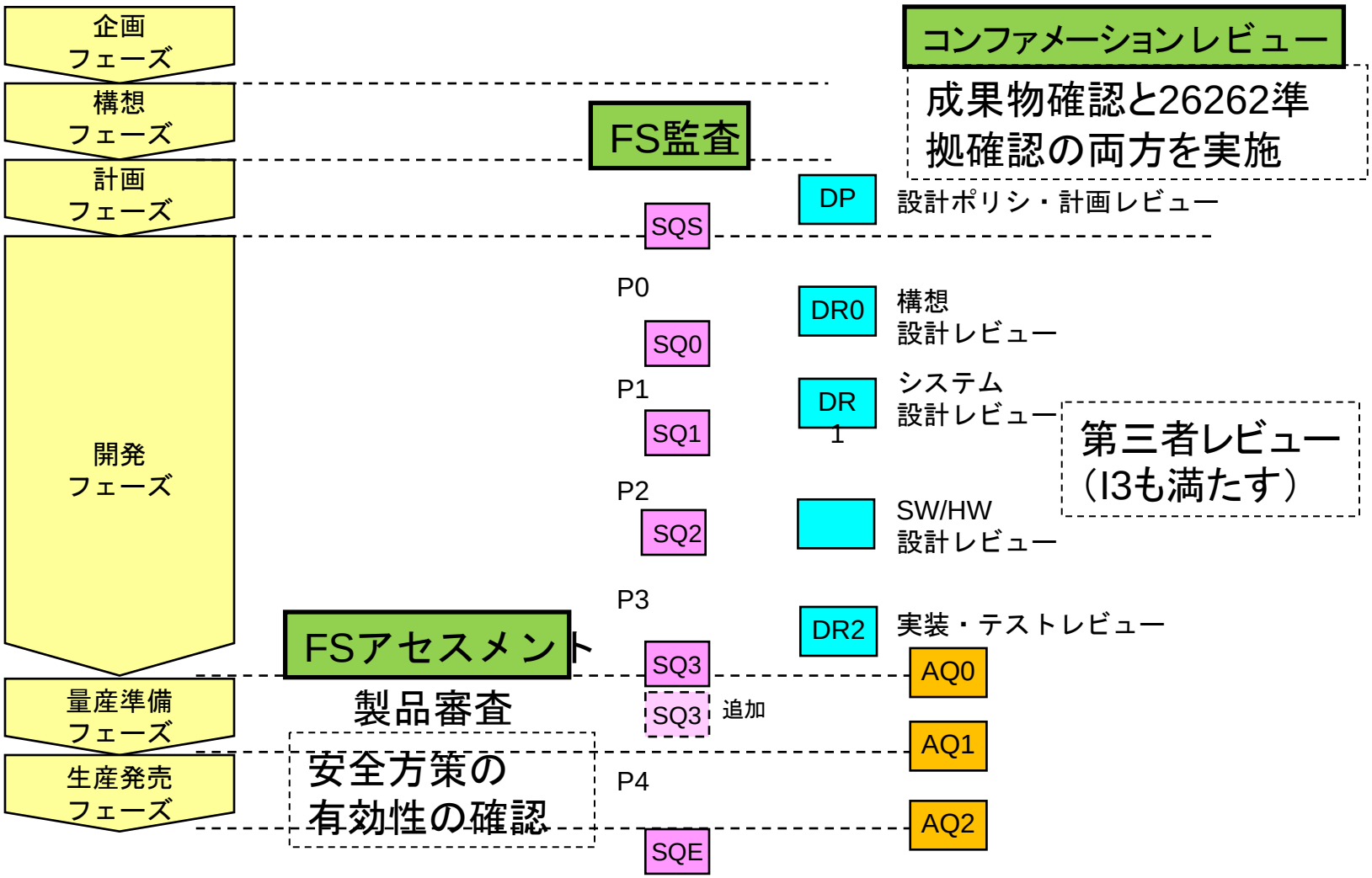
ルールは正しく使用され、遵守されてるか

対象はソフト、ハード両方

既存の開発ライフサイクルのイベントに割り当て

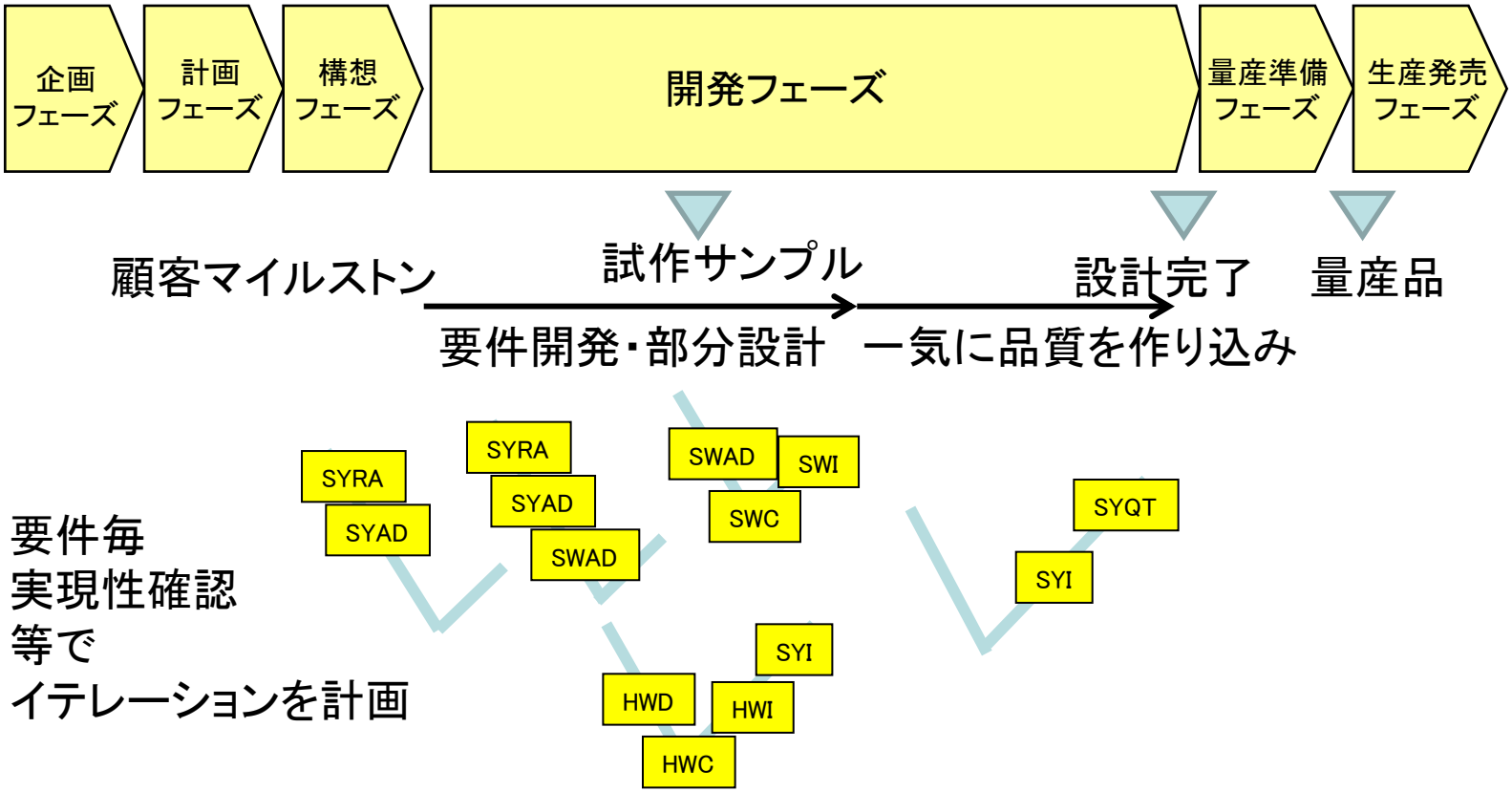
既存の開発イベントへの割り当て

Panasonic ideas for life



従来の移行承認ゲートに割り当てる

反復計画



顧客サンプル納入や内部イベントに合わせて、実施するプロセスやアクティビティを選択して小さなVを何度も回すプロセスアプローチは現実的な開発を実現。

従来の考え方を踏襲

ソフトウェアツールの適格性確認

Panasonic
ideas for life

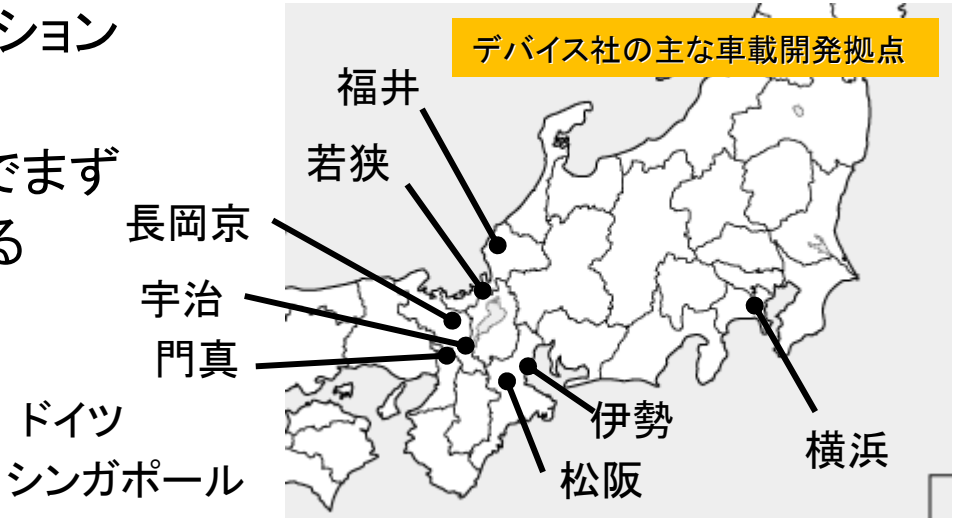
- 組織レベルで使用するツールを統一
  - ユースケースを明示し、ツールの適格性を評価
- 適格性確認結果はプロジェクトで共有

過去からツールは社内で統一

専門チームによるサポート

Panasonic ideas for life

- 機能安全規格がわかる技術者の育成
  - 機能安全規格と機能安全プロセスのわかる技術者の育成～出前研修による全員教育
- 機能安全規格が使える専門家の育成
  - まず3名の専門チームメンバーが専門家になる
    - SW,HWの製品開発を経験
  - パナソニック全社に機能安全WGを設立。
    コアメンバーとのディスカッション
    による切磋琢磨！
  - パイロットの実プロジェクトでまず
    は、機能安全活動の形を作る
  - OJTで専門家を作っていく
  - ASIL適用プロジェクトが
    増える前に先手



ノウハウの横展開が重要

機能安全スキル向上

Panasonic ideas for life

- 機能安全トレーニング
  - スキル認定ガイドラインにて必要スキルを明示
  - 車載用機能安全製品開発コース（1日）
    - 規格の教育と演習（安全コンセプトとハードウェアのメトリクス算出
  - システム製品開発プロセスコース（半日）
    - 機能安全対応プロセスを教える
  - 全車載開発担当者の教育を目指す（2012/4開講）

安全文化形成

- 機能安全エンジニアリングスキル立ち上げ
  - 安全コンセプト形成のコンサルティング

※デバイス社の技術講座

専門チーム（機能安全推進チーム）による対応

研修で広く網をかけ、コンサルで個別育成

コンサルティングによりできたこと

Panasonic ideas for life

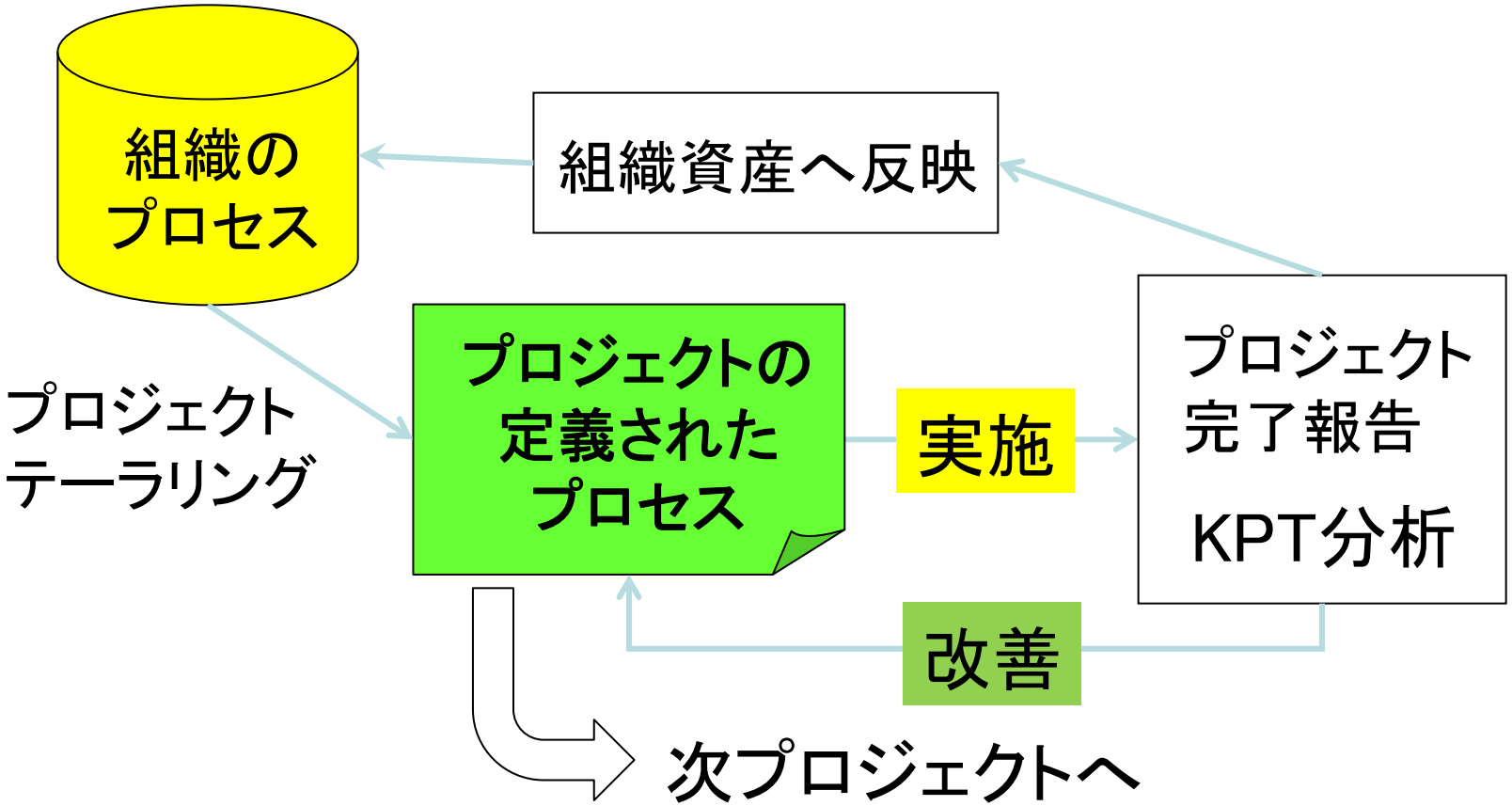
- 機能安全活動の形がわかってきた
  - 安全分析と技術安全コンセプト形成
  - 故障率計算
  - 安全プロセスの実施
  - コンフォーメーションメジャーの実施
  - ソフトウェアツールの適格性確認
- 苦労している点
  - ハードウェア技術者の巻き込みが難しい（特にPart4、Part5）
    - 安全方策は従来のフェールセーフである程度満足
    - それを、第三者にわかる形に書かせることに難航
      - **安全関連・非安全関連のエレメントの明確な分離**
      - **インタビューによる、主機能と安全メカニズムの分離**
      - **安全分析結果を関連づけた技術安全コンセプト形成**
    - **IEC62380ベースの故障率計算とDCのアーギュメント**
  - ソフトウェア技術者の巻き込みはスムーズ
    - Part6、Part8（一部を除く）はAutomotiveSPICEの要求に近い

専門チームメンバーも現場と共に学び、機能安全活動の形を確立し、横展開
Panasonic社内の他の事例を担当しているメンバーと情報交換と共通解釈

改善活動による効率化を目指す

Panasonic ideas for life

自律改善・継続改善の重要性



目指す姿はここ。自ら考え、効率化