車載ソフトウェア搭載製品の機能安全監査と審査

2012年10月11日

パナソニック株式会社　デバイス社

菅沼　由美子

パナソニックのデバイス製品

パナソニックは、さまざまなデバイス&コンポーネンツを“Total Solution”で提供いたします。

Panasonic provides "Total Solutions" through various components and devices.

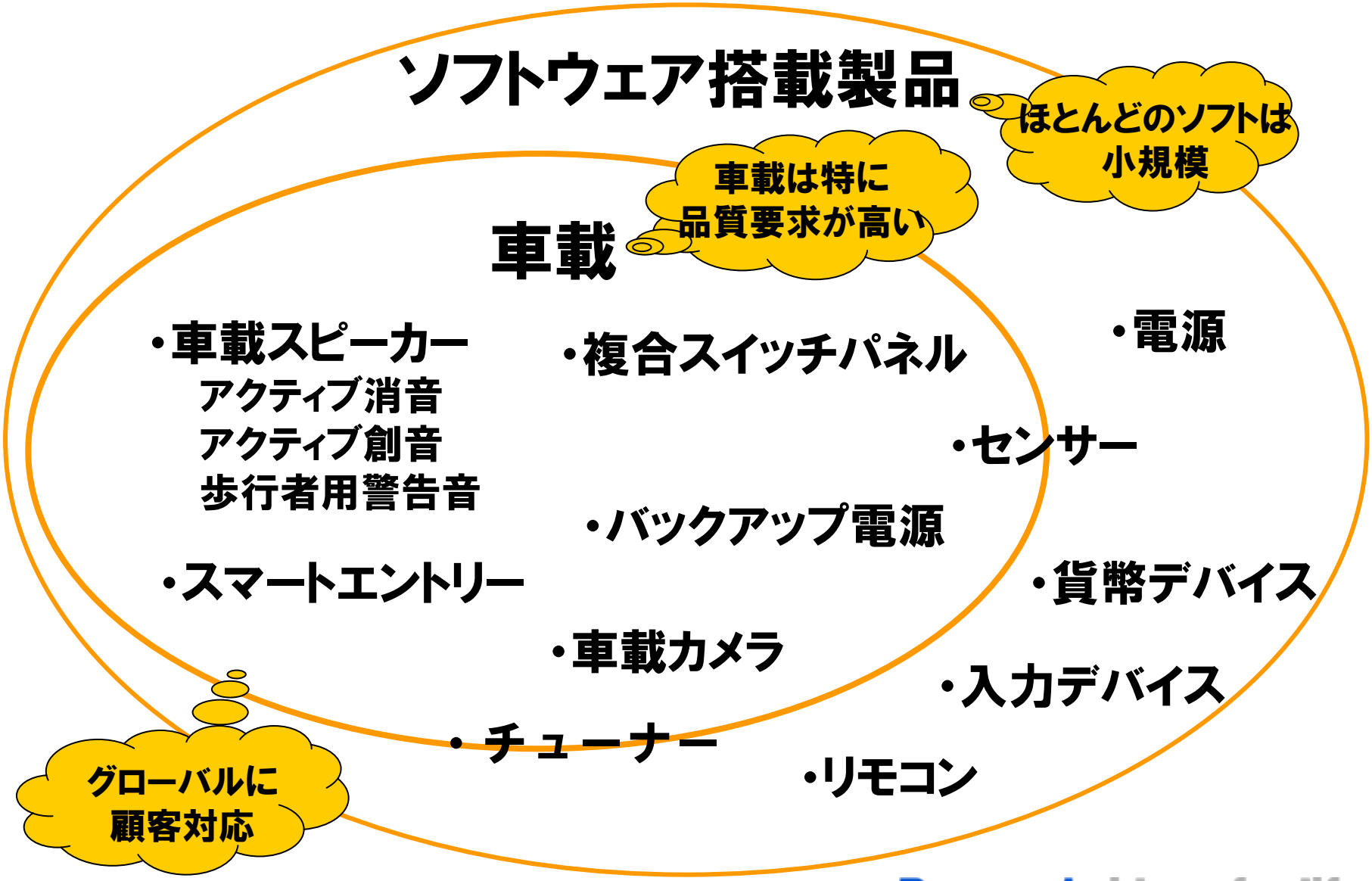
Panasonic将以独有的“整体解决方案”为客户提供各种各样的元器件和组件。

半導体から、デバイス・部材にいたるまでパナソニックのお届けしている生産財は多種多様です。
いわば“One Stop Shop”で、しかもグローバルな“One Window”の販売プラットフォームにより、
トータルソリューションを提供いたします。

Panasonic delivers a wide range of products used in production,
from semiconductors to devices and materials.
We contribute to your business development using our "One Stop Shopping" or
even our "One Window" global sales platform.

Panasonic ideas for life

パナソニック㈱デバイス社のソフト搭載製品



車載部品への機能安全要求

車載部品への機能安全の要求(ISO26262)

故障のリスクを下げる

その上、顧客要求は、
短納期化、複雑化

故障とは

システマティック故障

開発の工程の作業成果に原因がある故障

開発プロセス定義、作業者のスキル強化、組織間の連携強化

ソフトウェアやハードウェア(回路)設計

ランダムハードウェア故障

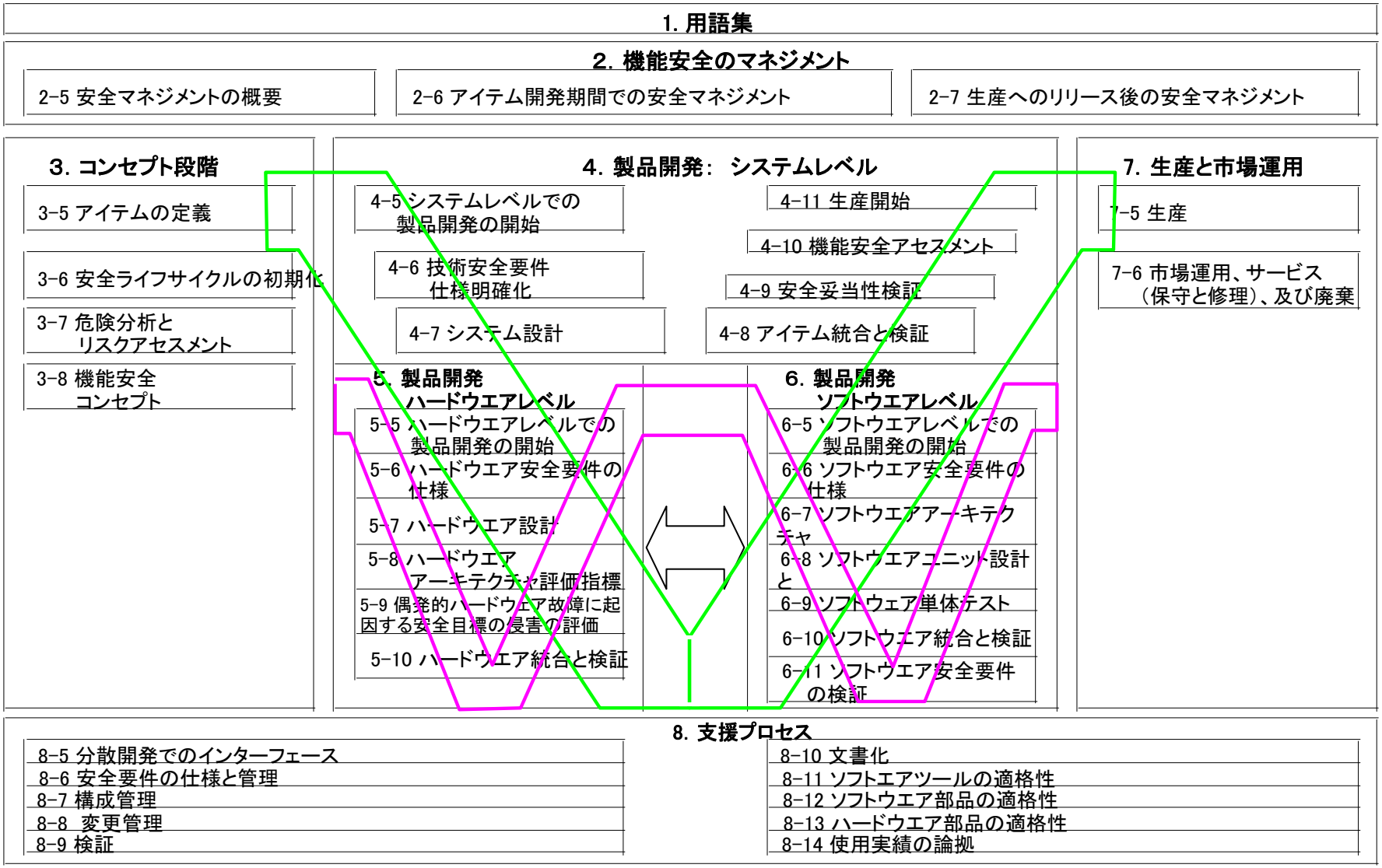
構成部品の劣化による時間的に無秩序の発生する故障

機能の冗長化、多重化、構成部品の故障検出

ハードウェア部品

安全関連の開発プロセスを規定(SYS,HW,SW)

ISO26262の構成



ISO26262で要求される確証方策

ISO26262 Part2 表1

確証方策 Confirmation measures	確認対象	デバイス社での 実現方法
確証レビュー Confirmation review	ハザード分析、リスクアセスメント、安全計画、安全解析、安全ケース、等	第三者による 技術レビュー
機能安全監査 Functional safety audit	・機能安全プロセスの実施	SQA監査
機能安全 アセスメント Functional safety assessment	・安全計画に計画された成果物 ・機能安全プロセスの実施 ・安全方策の適切性,効率性	審査

“機能安全”監査で実施すること

「機能安全プロセスの実施」の確認

…システム開発プロセス監査

◆対象プロセス

…システム、ハード、ソフト

◆プロセスに定義された、機能安全の要求事項の実施を確認する

ところで…監査には何が必要？

◆監査の前に

①目的を満たせるプロセスがある…規程、基準、ガイドライン、etc　①②
②プロジェクトがプロセスを知っている…トレーニング
③プロジェクトがプロセスを使っている…組織のコミットメント、レビュー　③
（エビデンスが有る）

◆監査の仕組み

④監査チェックリスト…チェック項目、判断基準　④
⑤監査員のスキル、工数…スキル要件定義、トレーニング体系・実施　⑤
監査組織のコミットメント
⑥監査員の権限…しくみ、マネジメントのコミットメント　⑥

◆監査時に

⑦対象プロジェクトの監査対象プロセス、成果物が分かる　⑦

◆更に

・ノウハウの蓄積
・第三者レビュー、監査、審査の連携

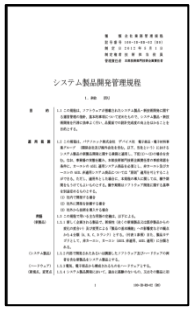
審査

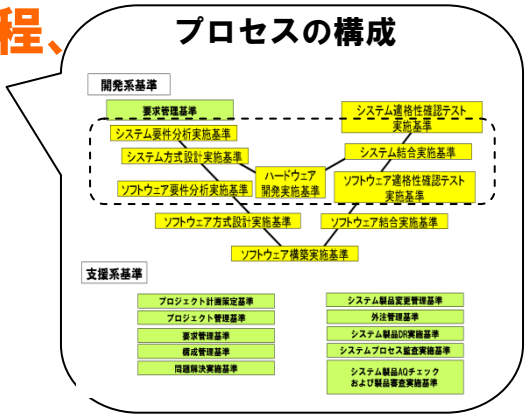
システム製品開発プロセス

★機能安全
★短納期化
★複雑化

対応

システム製品開発管理規程、関連実施基準、ガイドライン、テンプレート、チェックリスト

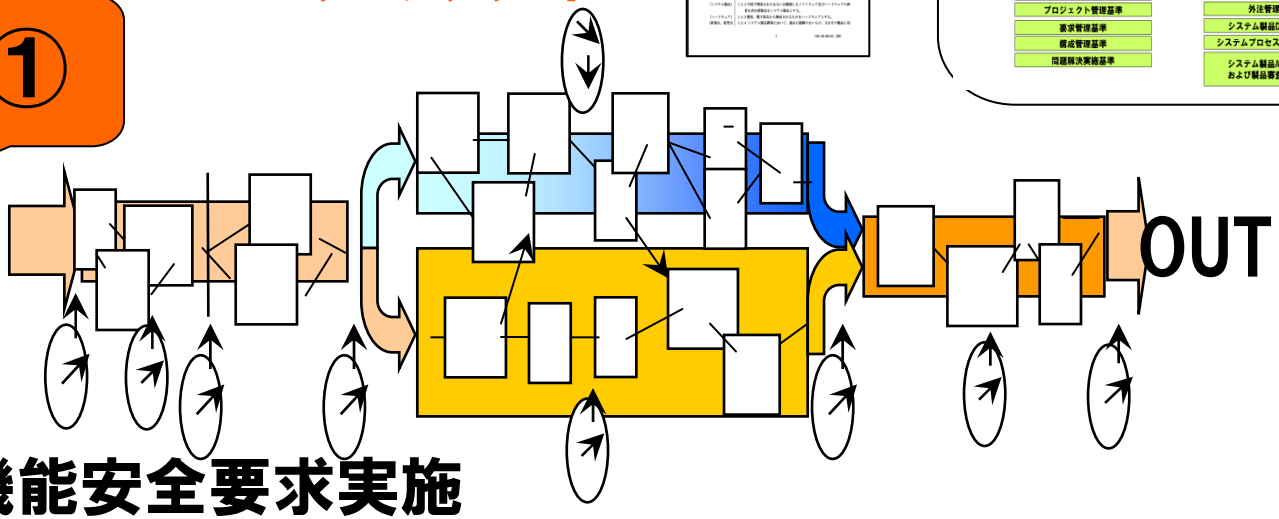




プロセス認証

①

IN



OUT

- 機能安全要求実施
- SYS/HW/SW整合強化
- エビデンス強化

の仕組み

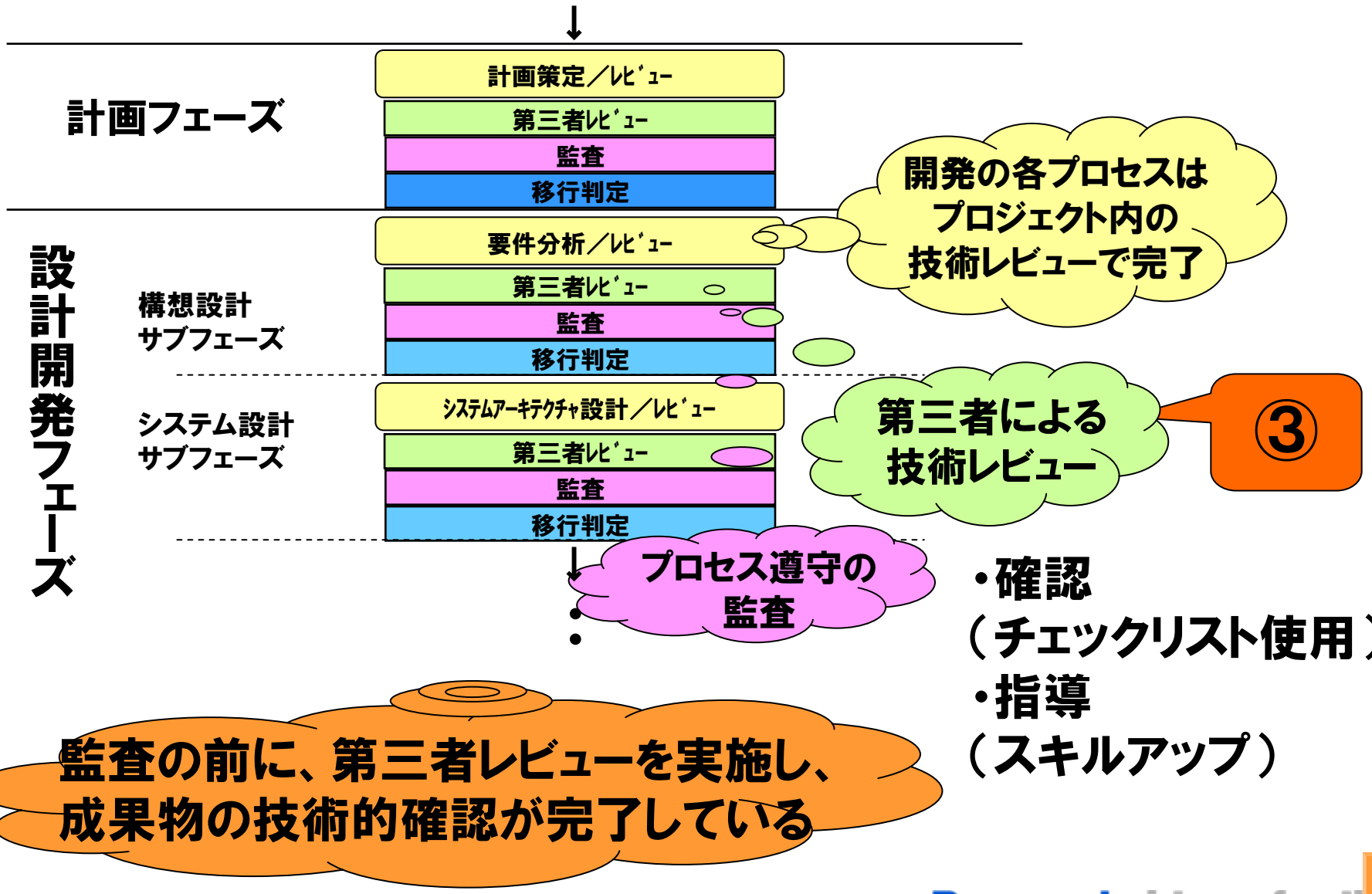
②

ID社技術講座2012

区分	【セミナー記号】	講座名	定員	日数	受講料（千円）	2011年 4-5月	6-7月	8-9月	10-11月	2012/ 12-1/
ヒューマンスキル	T 741	技術者のファシリテーション	20	1	~15			8/31（金）	職場コミュニケーションの円滑化	
PM実践知識	T 703	プログラムマネジメント	30	1	~15		6/1（金）	プロマネ、管理		
プロセス開発	T 744-01,02	車載用機能安全製品開発コース	5~30	1	無料	5/18（金）			11/16（金）	
	T 745-01,02	システム製品開発プロセスコース Curis申請可	30	PM半日	無料		7/20（金）	＝開発プロセス／機能安全＝（関内容と狙い／年開催）		12/2（金）

トレーニング新設

レビューと監査の関係


計画フェーズ
計画策定／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
移行判定
設計開発フェーズ
構想設計
サブフェーズ
要件分析／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
移行判定
システム設計
サブフェーズ
ｼｽﾃﾑｱｰｷﾃｸﾁｬ設計／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
移行判定
開発の各プロセスは
プロジェクト内の
技術レビューで完了
第三者による
技術レビュー
③
プロセス遵守の
監査
・確認
（チェックリスト使用）
・指導
（スキルアップ）
監査の前に、第三者レビューを実施し、
成果物の技術的確認が完了している

監査チェックリスト（機能安全含む）

監査チェックリスト

第三者レビューで確認されているが、監査でも抜き取り確認する

④

機能安全の詳細観点

記載箇所 Base on	要求番号 Req. ID		要求事項 check items	監査時のチェック内容	実施基準 A	B	C	D	作業 work p
(SRDG) 5.1 機能安全要求の導出	FS3-8.4.2.1	1	機能安全要求は、初期のアーキテクチャを考慮し、安全目標と安全状態より導出されなければならない。		++	++	++	++	安全コンセプ functional sa specification
	FS3-8.4.2.2	1	各安全目標に対して、少なくとも一つの機能安全要求が特定されなければならない。		++	++	++	++	安全コンセプ functional sa specification
	FS3-8.4.2.3		各機能安全要求は、適用できる場合は、以下の情報を考慮して特定しなければならない。		–	–	–	–	安全コンセプ functional sa specification
		1	a) 運転モード		++	++	++	++	
		2	b) フォールトトレラント時間間隔		++	++	++	++	
		3	c) 安全状態		++	++	++	++	
		4	d) 緊急の運転の間隔		++	++	++	++	
			性		++	++	++	++	
	4.2.4	1	もし、安全可能な時間間隔に、運移によって安全状態に到達しないならば、緊急運転が特定されなければならな		++	++	++	++	安全コンセプ functional sa specification
	FS3-8.4.2.5	1	警告とデグラデーションのコンセプトは、機能安全要求として特定されなければならない。		++	++	++	++	安全コンセプ
	FS3-8.4.2.6		もし、安全目標に準拠するために、仮説が、運転者もしくは他の危険にさらされる可能性がある人の必要な活動に		–	–	–	–	

何に関する機能安全要求があるかと、参照するガイドラインを記載

成果物のテンプレート（どこに何が記載されるか）が決まっているので、確認が容易

具体的な確認事項：

記載例…
「○○設計書の△△章に◇◇が記載されている」

SQAのスキルマネジメント

⑤

SQAのスキル要件：このレベルがないと監査できない
トレーニング体系：スキルレベルを得るのに必要な研修
…ここに、機能安全を追加

HW関連も整備中

民生プロジェクトの SQAの要件

車載プロジェクトのSQAの要件

監査活動監査員の要件

2012年度 PED-SQA
スキル要件とトレーニングマップ

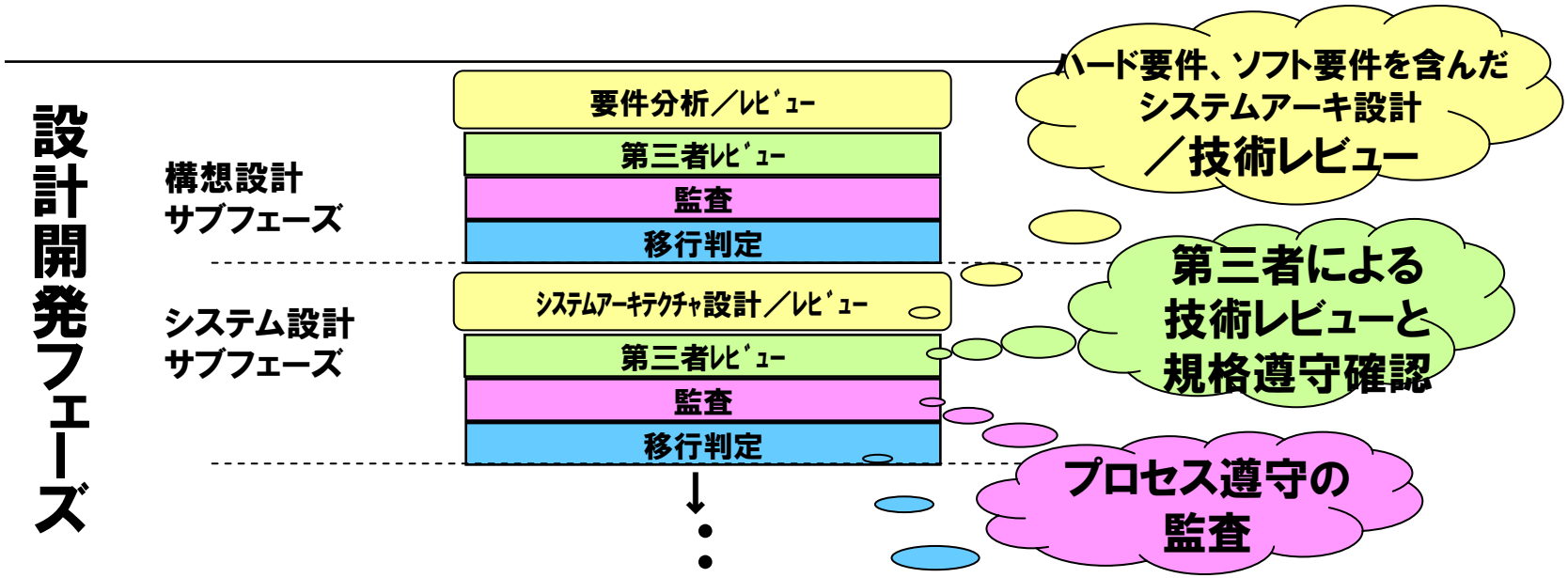
トレーニング対象 氏名 | 作成 | 承認

スキル要件	スキルレベル	レベル1	レベル2	レベル3	レベル4	レベル5	レベル6
	担当できるSQA監査業務	量産開発以外（下記プロジェクト区分②）の監査を担当できる	車載以外の組込みシステム（量産開発）の監査を担当できる	車載組込みシステム（量産開発）の監査を担当できる ただし、カーエレキスパートSQAの「ゴールド」を取得すること	PED内SQA監査活動の監査を担当できる	監査実施に対する改善指導が出来る	―
	知識・知見 SQA業務指針10業務の実践スキル	PEDシステム開発標準の概要を理解している。	PEDシステム開発標準の詳細と、SQA業務指針概要を理解しており、上位者の指示の下、最優先4項目（下記 1-4）を実施できる。	PEDシステム開発標準の詳細に精通、ソフトウェア開発プロセスの知識が豊富で、最優先4項目を主体的に実施できることに加え最優先3項目（下記 5-7）を上位者の支援の下実施できる。	ソフトウェア開発・技術・手法、品質管理・保証に関する専門知識が豊富で、最優先・優先7業務を主体的に実施できることに加え、残り3項目に関してもある程度実施可能。	SQA業務手順を組織の基準や手順への落としこみ、改善ができる。	
	PEDソフト搭載システムの監査経験	★PEDの量産開発以外の監査への参加経験有り。（監査メンバー、又は、オブザーバー）	★PEDの量産開発以外の監査実施経験有り。 または ★PEDの車載以外の組込みシステムの監査への参加経験有り。（監査メンバー）	★PEDの車載以外の組込みシステム（量産開発）の監査実施経験有り。 または ★PEDの車載組込みシステムの監査への参加経験有り。（監査メンバー）	★PEDの車載組込みシステム（量産開発）の監査実施経験有り。 または ★PED内SQA[illegible]有り。	[illegible]する者で、[illegible]動を発表できる。	
	PASSPORTアセスメント	―	☆PASSPORTアセスメント参加経験あり	★PASSPORTアセッサ補以上の資格を有する			

トレーニングマップ	スキルレベル / 分野	レベル1までに受講 研修名（開催組織）	計画	実績	レベル2までに受講 研修名（開催組織）	計画	実績	レベル3までに受講 研修名（開催組織）	計画	実績
	品質保証／品質管理全般	☆PEDスキルチャレンジ大学品質学部			☆(CR302)品質管理基礎(HRDC)			☆(CM198)DRBFM活用による実践的設計検証法（HRDC）		
	ソフトウェア品質保証（SQA）				★SQA新任研修（技品本部）			★SQA初級研修[illegible]		
					★(CS020)SQAによる監査とレビュー（HRDC, PID技術講座）			★(CS014)[illegible]証入門(HRDC)		
	エンジニアリング／安全				★(CS011)ソフトウェア開発入門(HRDC)			★(CS010)ソフトウェアせな[illegible]（HRDC or PID技術講座）		
					☆(CS012)基礎から学ぶソフトウェアテスト(HRDC)			★機能安全研修（PID技術講座）		
	ソフトウェア（システム）開発プロセス				★開発プロセス概論（SEC/技品本部）			★（CD002）「PASSPORT アセッサ能力開発」(HRDC)		
					☆(CD001)CMMI基礎(HRDC)			★（CD003）「PASSPORT アセスメント実践」(HRDC)		
					☆(CD0054)「パナソニック ソフトウェア開発プロセスガイドライン」の活用法（HRDC）			☆Automotive SPICE（独習） ※欧州顧客対応の場合は必須		
	PEDソフトウェア開発プロセス	★PEDソフトウェア開発プロセス概論（QIC or DSDC）			★PEDシステム開発プロセスとプロセス品質管理表（QIC）			★車載顧客要求事項（QIC or DSDC）		
		★SQA監査（QIC）			★構成管理とベースラインチェックリスト（QIC）					

ただし、監査の仕組み：
・第三者レビュー結果の参照、
・詳細チェックリスト
により、監査の難易度と監査員の必要スキルを下げている

監査とマネジメントレビュー



・第三者レビュー結果

・プロセス監査結果

移行判定：
マネジメントレビュー

⑥

を、移行判定会議（マネジメントレビュー）の入力とする

マネジメント層へのエスカレーション

監査対象プロセス・成果物

監査チェックリスト

プロジェクトの計画に合わせて監査対象プロセスを選択

⑦

スケジュール Schedule

フェーズとステージ

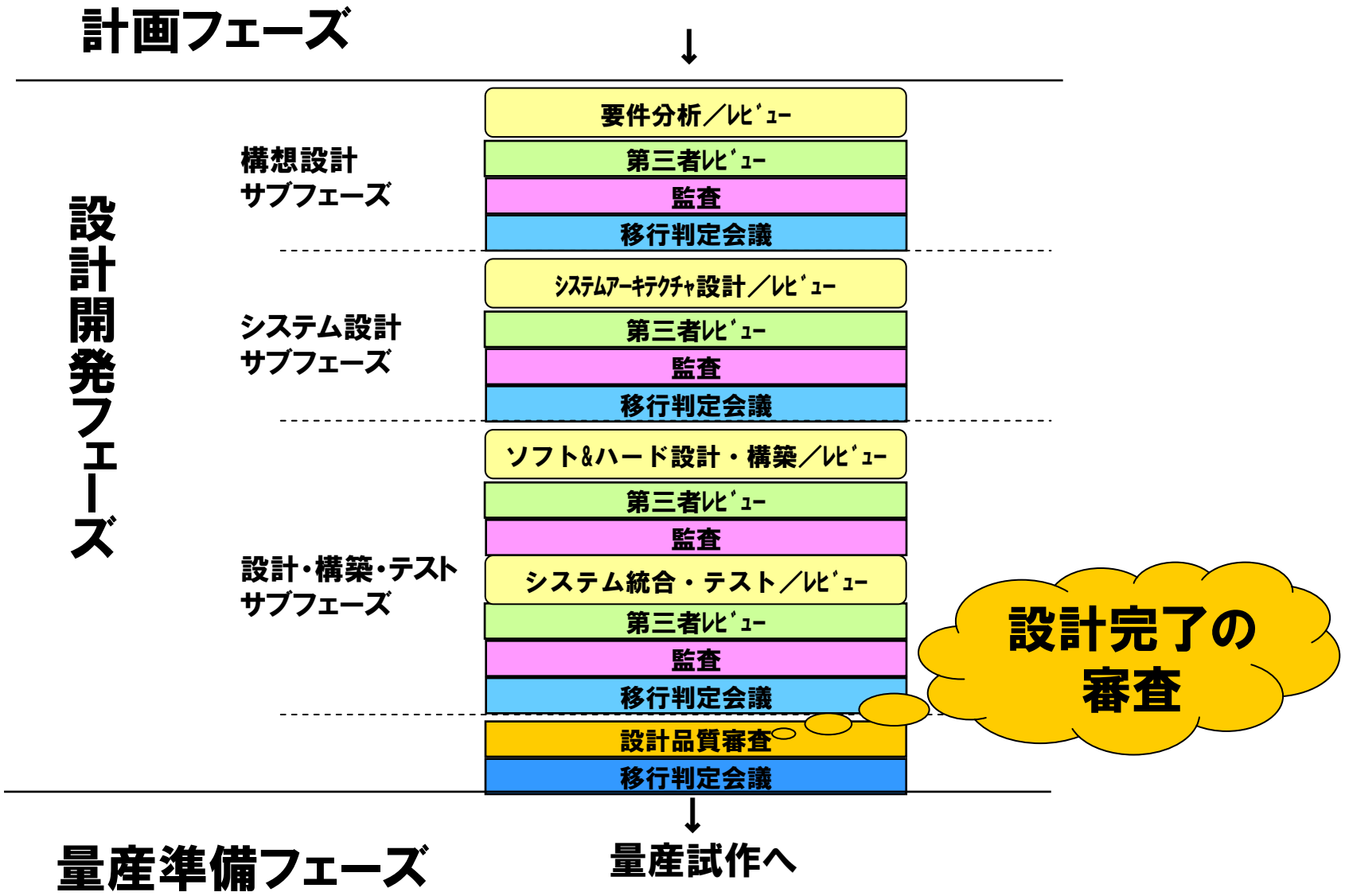
実施するプロセス

プロジェクト計画書のスケジュール表

構成管理計画

作成・変更した成果物

審査のタイミング


計画フェーズ
設計開発フェーズ
構想設計
サブフェーズ
要件分析／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
移行判定会議
システム設計
サブフェーズ
ｼｽﾃﾑｱｰｷﾃｸﾁｬ設計／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
移行判定会議
設計・構築・テスト
サブフェーズ
ソフト&ハード設計・構築／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
システム統合・テスト／ﾚﾋﾞｭｰ
第三者ﾚﾋﾞｭｰ
監査
移行判定会議
設計品質審査
移行判定会議
設計完了の
審査
量産準備フェーズ
量産試作へ

機能安全審査で実施すること

- ◆「安全計画に計画された成果物」の確認
  - ◆第三者レビュー結果と、レビュー方法の適切さを確認
  - ◆26262規格要求の遵守
- ◆「機能安全プロセスの実施」の確認
  - ◆機能安全監査の結果と、監査方法の適切さを確認
- ◆「安全方策の適切さと有効性」の確認
  - ◆妥当性確認を実施

第三者レビューと連携

機能安全監査と連携

機能安全の視点を強化

機能安全審査員のトレーニングコース整備中

まとめ

- 従来のソフトウェアの監査の仕組みを拡張し、システム、ハード、ソフトの開発プロセス遵守を保証する監査の仕組みを構築。
  - この仕組みにより、機能安全監査を実施可能にした。
- 機能安全審査の仕組みを構築。

- 今後の取り組み
  - ・機能安全監査のノウハウ蓄積
  - ・機能安全審査のノウハウ蓄積
  - ・監査、審査、第三者レビューの、連携の更なる強化

ご清聴ありがとうございました

Panasonic

ideas for life