

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

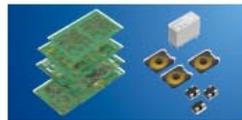
パナソニックは、さまざまなデバイス&コンポーネントを
 “Total Solution” で提供いたします。

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.



回路部品・接続部品・プリント配線板

Passive & Electromechanical, Switches, Printed Wiring Board

电阻等部品、连接器件、印刷电路板



- 抵抗器
- コンデンサ
- インダクタ(コイル)
- スイッチ
- フィルタ
- EMI/RF部品
- コーシスタ
- プリント配線板
- カーエレクトロニクスデバイス
- リレー
- コネクタ
- 自動車デバイス
- MIPTEC
- Resistors
- Capacitors
- Inductors
- Switches
- Filters
- EMI Components
- Fuses
- Thermistors
- Printed Wiring Board
- Devices for Car Electronics
- Relays
- Connectors
- Automotive Devices
- MIPTEC



表示入出力デバイス・通信・センサ

I/O Devices, Communication Units, Sensors

显示及输入输出器件、通讯、传感器



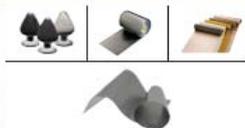
- ディスプレイ
- センサ
- 音声ネットワークユニット
- 音声部品
- 入出力ユニット
- 光学部品
- オプティカルイメージングユニット
- 産業用インクジェット
- 産業用センサ
- カードリーダー
- Display
- Sensors
- IP/Network Units
- Acoustic Components
- Input/Output Units
- Optics Components
- Optical Imaging Unit
- Industrial Inkjet Head
- Built-in Sensors
- Card Reader



素材・材料

Materials

材料



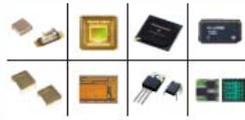
- 半導体封止材
- アフスタック成形材料
- アフスタック成形成形品
- 電子回路基板材料
- プレキシール基板材料
- 積層フィルム
- PGSタフファイトシート
- シールドシート
- Semiconductor Encapsulation Materials
- Plastic Molding Compounds
- Precision Molding Plastic Products
- Circuit Board Materials
- Flexible Circuit Board Materials
- Advanced Films
- PGS Graphite Sheet
- Shield Films



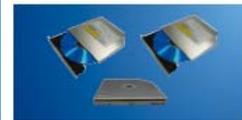
半導体

Semiconductors

半导体



- マイクロコンピュータ
- 画像撮取り
- 専用IC
- センサ
- GaAsデバイス
- トランジスタ
- 複合デバイス(クリート)
- ダイオード
- 光半導体
- フラッシュメモリデバイス
- ハイブリッドIC
- Microcomputers
- Image Pickup Devices
- Application-Specific Standard-Product ICs
- Sensors
- Gallium Arsenide Devices
- Transistors
- Multi-Chip Discrete Devices
- Diodes
- Opto Electronic Devices
- Solid State Devices
- Hybrid IC



記憶デバイス

Storages, Supplies

存储器件



- スーパーマルチドライブ
- ブルーレイディスクドライブ
- メディア
- Super Multi Drives
- Blu-ray Disc Drives
- Media



FA(産業用)デバイス

Factory Automation Devices

工厂自动化设备



- FAセンサ
- レーザマーカ
- プログラマブルコントローラ
- 画像処理機
- プログラマブル表示器
- フォトカーテン(安全センサ)
- エネルギー管理機
- FAコンポーネント
- FA Sensors
- Laser Markers
- Programmable Controllers
- Machine Vision Systems
- Programmable Displays
- Light Curtains
- Energy Consumption Visualization Components
- FA Components



電源・電池・エネルギー機器

Power Supplies, Batteries & Energy Products

电源・电池・能源设备



- 電源ユニット
- 蓄電池(鉛蓄電池)
- リチウムイオン電池
- ニッケル水素電池
- 鉛蓄電池
- リチウム・マイクロリチウム
- アルカリ電池
- Power Supply Units
- Power Circuit Components
- Lithium ion Batteries
- Nickel Metal Hydride Batteries
- Lead Acid Batteries
- Lithium & Micro Batteries
- Zinc Carbon Batteries



モータ・コンプレッサ

Motors, Fans, Compressors

马达、风扇、压缩机



- FA一般産業用モータ
- 家庭用・産業用モータ
- 高効率デバイス
- ポンプ
- コンプレッサ
- Motors for FA, Industrial Application
- Motors for Home Appliances
- Cooling Devices
- Pumps
- Compressors

■ パナソニックグループ会社で開発、製造。 Developed and manufactured within other Panasonic group companies.

パナソニック(株)デバイス社のソフト搭載製品

ソフトウェア搭載製品

ほとんどのソフトは
小規模

車載は特に
品質要求が高い

車載

- ・車載スピーカー
アクティブ消音
アクティブ創音
歩行者用警告音

- ・複合スイッチパネル

- ・電源

- ・センサー

- ・バックアップ電源

- ・スマートエントリー

- ・貨幣デバイス

- ・車載カメラ

- ・入力デバイス

- ・チューナー

- ・リモコン

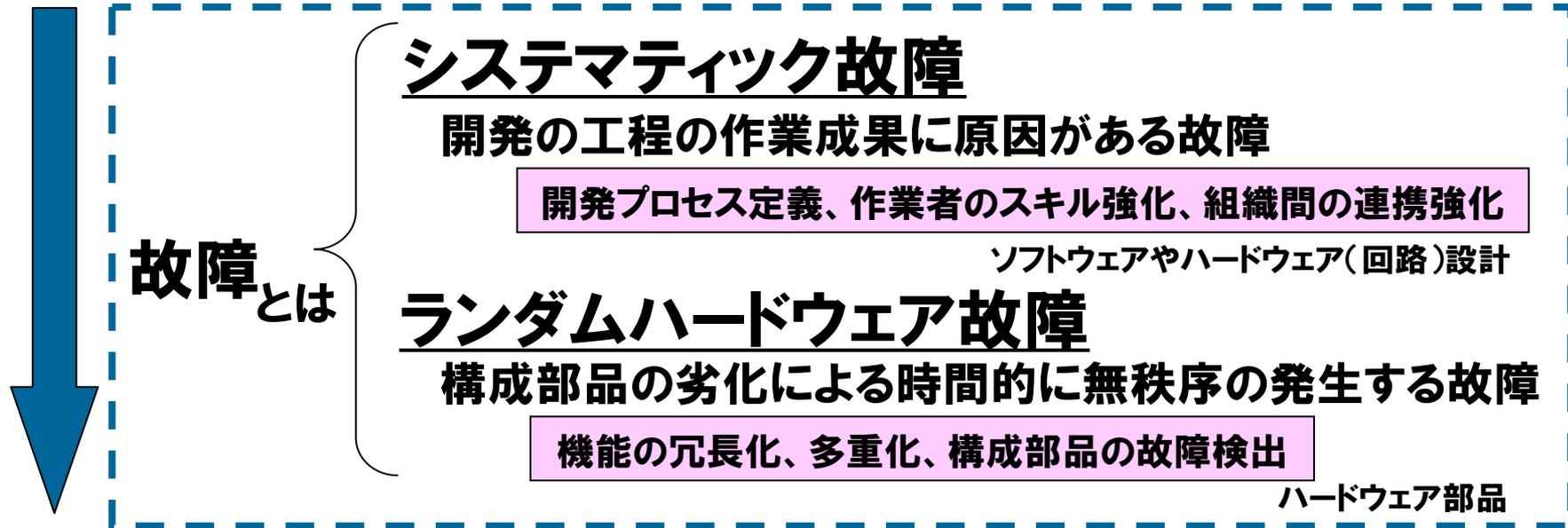
グローバルに
顧客対応

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



安全関連の開発プロセスを規定 (SYS,HW,SW)

ISO26262の構成

1. 用語集

2. 機能安全のマネジメント

2-5 安全マネジメントの概要

2-6 アイテム開発期間での安全マネジメント

2-7 生産へのリリース後の安全マネジメント

3. コンセプト段階

3-5 アイテムの定義

3-6 安全ライフサイクルの初期化

3-7 危険分析と
リスクアセスメント

3-8 機能安全
コンセプト

4. 製品開発：システムレベル

4-5 システムレベルでの
製品開発の開始

4-6 技術安全要件
仕様明確化

4-7 システム設計

4-11 生産開始

4-10 機能安全アセスメント

4-9 安全妥当性検証

4-8 アイテム統合と検証

7. 生産と市場運用

7-5 生産

7-6 市場運用、サービス
(保守と修理)、及び廃棄

5. 製品開発 ハードウェアレベル

5-5 ハードウェアレベルでの
製品開発の開始

5-6 ハードウェア安全要件の
仕様

5-7 ハードウェア設計

5-8 ハードウェア
アーキテクチャ評価指標

5-9 偶発的ハードウェア故障に起
因する安全目標の侵害の評価

5-10 ハードウェア統合と検証

6. 製品開発 ソフトウェアレベル

6-5 ソフトウェアレベルでの
製品開発の開始

6-6 ソフトウェア安全要件の
仕様

6-7 ソフトウェアアーキテク
チャ

6-8 ソフトウェアユニット設計
と

6-9 ソフトウェア単体テスト

6-10 ソフトウェア統合と検証

6-11 ソフトウェア安全要件
の検証

8. 支援プロセス

8-5 分散開発でのインターフェース

8-6 安全要件の仕様と管理

8-7 構成管理

8-8 変更管理

8-9 検証

8-10 文書化

8-11 ソフトウェアツールの適格性

8-12 ソフトウェア部品の適格性

8-13 ハードウェア部品の適格性

8-14 使用実績の論拠

9. ASIL(自動車安全度整合レベル)指向および安全指向の分析

9-5 ASILテーラリングに関する要件の分解

9-6 要素の共存のための基準

9-7 従属故障の分析

9-8 安全分析

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
- 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（エビデンスが有る）

①②

③

◆ 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
- 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
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

④

⑤

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

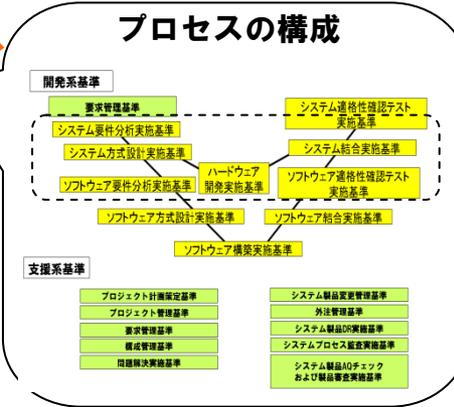
審査

システム製品開発プロセス

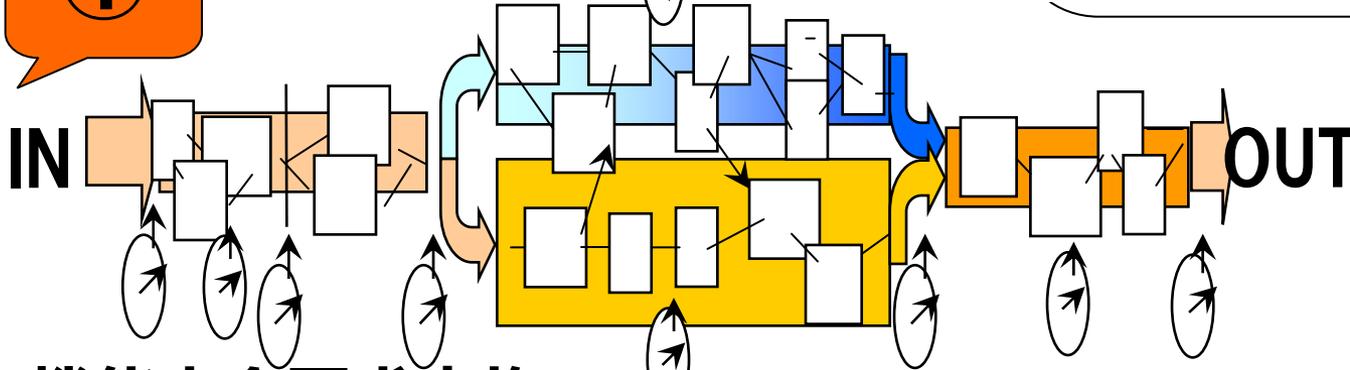
- ★機能安全
- ★短納期化
- ★複雑化



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



- ・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

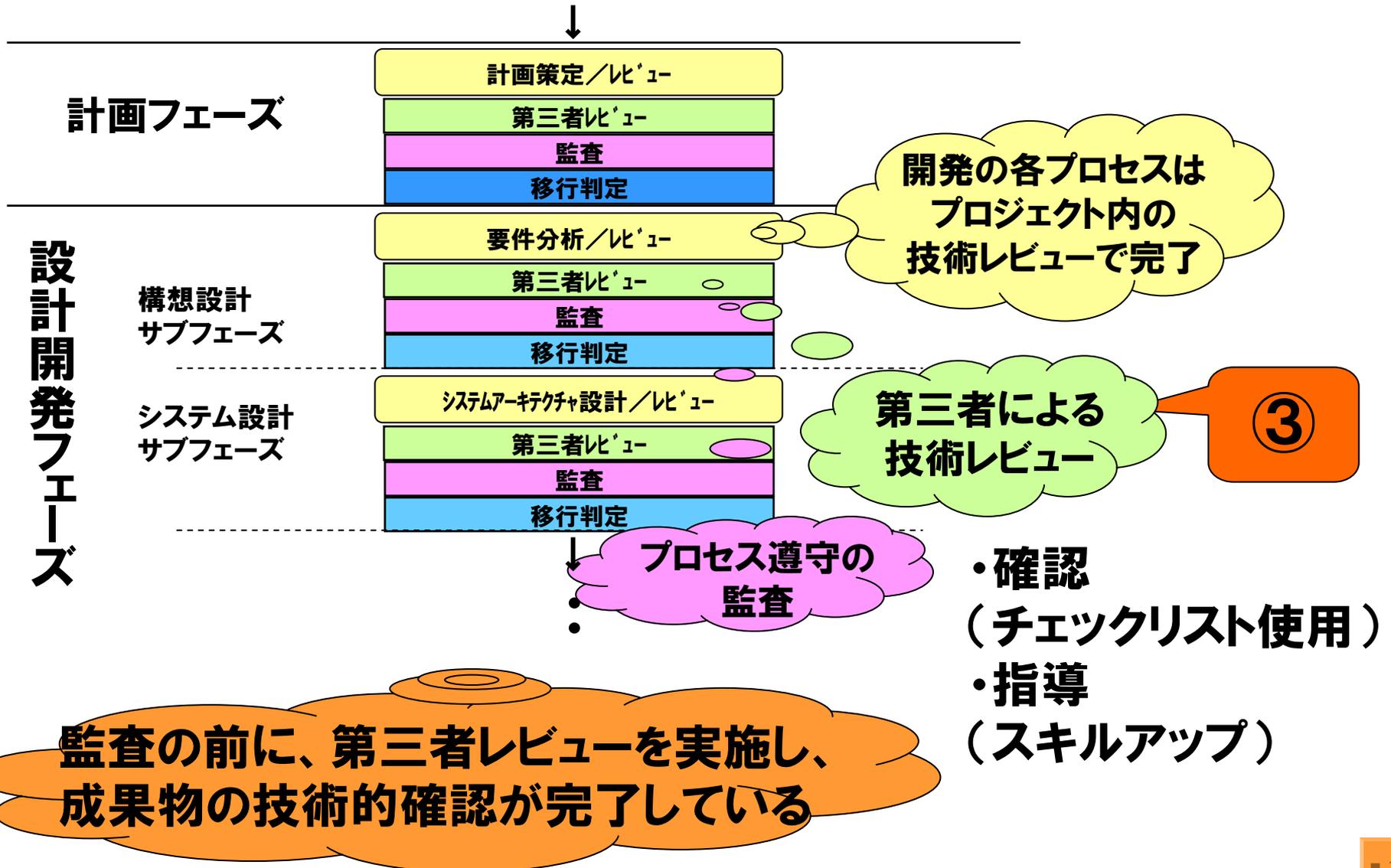
トレーニング新設

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 12-11
ヒューマン	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
P 実践知識	T 703	プログラムマネジメント	30	1	~15		6/1 (金)			プログラ、管理
プロ 開発 セス	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	30	PM 半日	無料		7/20 (金)			開発プロセス/機能安全 (両内各2回/年開催)



レビューと監査の関係



監査チェックリスト(機能安全含む)

4.3 プロジェクト管理	A				
5. プロジェクト開始 ← 構想DCPでの承認					
5.3 開発プロジェクト計画(5.4 安全計画)の立案					
5.7 SOS					
5.8 DP会議/ 5.9 企画決済/ 5.10 計画DCP					
6.1 構想設計					
6.1.1 要求のとりまとめ					
6.1.1 要求のとりまとめ(変更管理)	A				
6.1.2 構成管理の開始					
6.1.3 構想設計					
6.1.4 計画の詳細化					
6.3 SOO					
6.4 DRO					
6.5 システム設計					
6.5.1 システム要件開発					
6.5.2 システム適合性確認テスト仕様策定					
6.5.3 システム要件レビュー					
6.5.4 システムアーキテクチャ設計					
6.5.5 システムアーキテクチャの分析:FMEA					
6.5.5 システムアーキテクチャの分析:設計基準					
6.5.6 システム結合テスト仕様策定					
6.5.7 システムアーキテクチャ設計レビュー					
6.5.8 計画の詳細化					
6.8 SOT					
6.9 DR1					
6.10 ソフトウェア設計					
6.10.1 ソフトウェア要件分析	A				
6.10.1 ソフトウェア要件分析(テスト仕様)	A				
6.10.2 ソフトウェア要件分析レビュー	A				
6.10.4 ソフトウェア設計	A				
6.10.4 ソフトウェアコンポーネントの分析:FMEA	A				
6.10.4 ソフトウェアコンポーネントの分析:設計基準	A				
6.10.4 ソフトウェア設計(テスト仕様)	A				
6.10.5 ソフトウェア設計レビュー	A				
6.16					

担当者	入力成果物	出力成果物	承認者
SWENG	システムアーキテクチャ設計書、システム結合テスト仕様書、ソフトウェア要件仕様書、ソフトウェアFMEA(DRBFM)、設計基準確認結果(SWAD)チェックリスト、過去トラチェックリスト	ソフトウェアアーキテクチャ設計書	-

実施必須項目
1) SW要件確認] S 2) コンポーネント分析 3) インターフェース設計 4) 静的構造/動的 5) 権限の設計] C 6) 「一貫性・正確性」 7) 「データ構造の設計 見直し」] C 8) 「文書化」] SWAD
観点
1) 要件に関する課題を 1) 必要な開発環境が 2) ソフトウェア要件仕様 2) 新規/流用/輸入 2) 必要に応じて、設計
機能安全の観点
ソフトウェア要件の動 ソフトウェアの再利用は ソフトウェアが利用す ソフトウェア設計の設計 ソフトウェアレ

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				作業 work
				A	B	C	D	
(SRDG) 5.1 機能安全要求の導出	FS3-8-42.1	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
	FS3-8-42.2	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
	FS3-8-42.3	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。 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		-	-	-	-	安全コンセプ functional sa specification
	4.2.4	1) 安全可能な時間間隔に、遷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い。		++	++	++	++	安全コンセプ functional sa specification
	FS3-8-42.5	1) 警告とデklaration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 functional sa specification
	FS3-8-42.6	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		-	-	-	-	安全コンセプ functional sa specification

ポップアップ

チェック項目

観点

機能安全の観点

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」

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

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

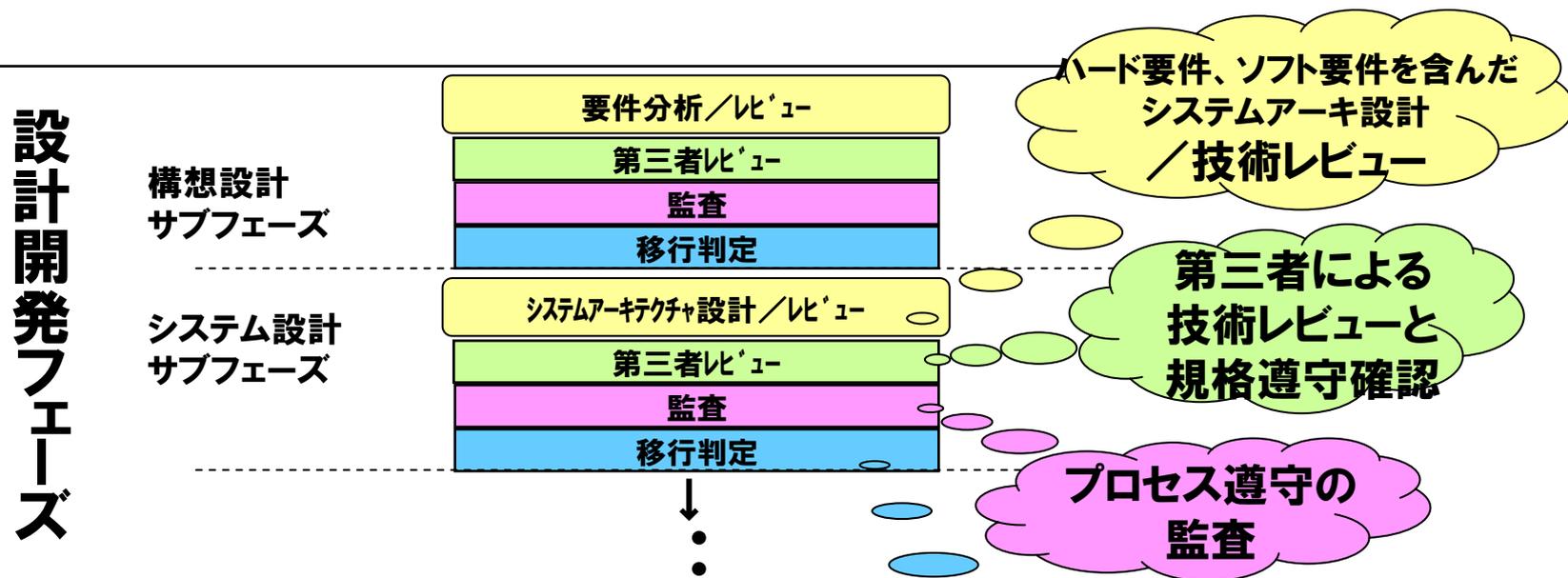
監査活動監査員の要件

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	車載開発以外(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(車載開発)の監査を担当できる	車載組込みシステム(車載開発)の監査を担当できる ただし、カーエレクトロニクスパートSQAの「ゴール」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業務の実務スキル	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、概観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、優先度4項目を主体的に実施できることに加え優先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、優先度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準拠し、改善ができる。				
PEDソフトウェアシステムの監査経験	*PEDの車載開発以外の監査への参加経験あり。(監査メンバー、又は、オブザーバー)	*PEDの車載開発以外の監査実施経験あり。 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あり。(監査メンバー)	*PEDの車載以外の組込みシステム(車載開発)の監査実施経験あり。 または *PEDの車載組込みシステムの監査への参加経験あり。(監査メンバー)	*PEDの車載組込みシステム(車載開発)の監査実施経験あり。 または *PED内SQA業務指針のゴール取得経験あり。					
PASSPORTアセスメント	-	*PASSPORTアセスメント参加経験あり	*PASSPORTアセスメント以上の資格を有する						
スキルレベル	レベル1までに受講		レベル2までに受講		レベル3までに受講				
分野	研修名(開催組織)	計画	実績	研修名(開催組織)	計画	実績	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			*CRS02)品質管理基礎(HRDC)			*GM198)IDRBM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(技本品庫)			*SQA初級研修(技本品庫)		
エンジニアリング/安全				*CS020)SQAによる監査とレビュー(HRDC, PD技術講座)			*CS014)組入門(HRDC)		
				*CS011)ソフトウェア開発入門(HRDC)			*CS010)ソフトウェアなぜなにの基礎(HRDC or PD技術講座)		
				*CS012)基礎から学ぶソフトウェアアタス(HRDC)			*機能安全研修(PD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/技本品庫)			*CD002)PASSPORTアセスメント概論(HRDC)		
				*CD001)CMMI基礎(HRDC)			*CD003)PASSPORTアセスメント実務(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(HRDC)			*Automotive SPICE(教習) ※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(QC or DSC)			*PEDシステム開発プロセスとプロセス品質管理(QC)			*車載顧客要求事項(QC or DSC)		
	*SQA監査(QC)			*機能管理とベースラインチェックリスト(QC)					

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

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



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/レビュー

第三者レビュー

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/レビュー

第三者レビュー

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/レビュー

第三者レビュー

監査

システム統合・テスト/レビュー

第三者レビュー

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

