

SQIP2012

システム、ハード、ソフト全プロセスに渡る

# システムプロセス監査の実施

～車載機能安全規格要求への対応～

2012年9月14日

パナソニック株式会社 デバイス社

電子部品・電子材料事業グループ

品質改革センター 品質保証グループ 設計品質チーム

菅沼 由美子

# 目次

- はじめに
- 自動車の機能安全
- ISO26262の要求
- デバイス社のシステムプロセス監査
- まとめ

# はじめに

- パナソニック(株)デバイス社のこと
- デバイス社のソフトウェア搭載製品

# パナソニックのデバイス製品

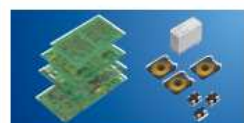
パナソニックは、さまざまなデバイス&コンポーネントを  
“Total Solution”で提供いたします。

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  
回路部品、接続部品、印刷配線板



■抵抗器  
■コンデンサ  
■インダクタ(コイル)  
■スイッチ  
■フィルタ  
■EMC対策部品  
■ヒューズ  
■サーモスタ  
■プリント配線板  
■カーエレクトロニクス  
■リレー  
■コネクタ  
■自動車デバイス  
■MPTEC  
■Resistors  
■Capacitors  
■Inductors  
■Switches  
■Filters  
■EMC Components  
■Fuses  
■Thermistors  
■Printed Wiring Board  
■Devices for Car Electronics  
■Relays  
■Connectors  
■Automotive Devices  
■MPTEC



## 表示入出力デバイス・ 通信・センサ

I/O Devices, Communication Units, Sensors  
表示及入出力用デバイス、通信・センサ



■ディスプレイ  
■センサ  
■音声ネットワーク  
■音響部品  
■入出力ユニット  
■光部品  
■オプティカル  
■イメージングユニット  
■産業用インジェクション  
■ビルドインセンサ  
■カードリーダー  
■Display  
■Sensors  
■RF/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

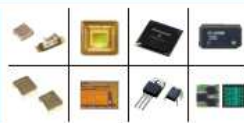


■半導体封止材  
■プラスチック成形材料  
■プラスチック成形材料  
■電子部品用樹脂材料  
■フレキシブル基板材料  
■有機EL材料  
■PGSグラファイトシート  
■シールドシート  
■Semiconductor Encapsulation  
■Materials  
■Plastic Molding Compounds  
■Precision Milled Plastic Products  
■Circuit Board Materials  
■Flexible Circuit Board Materials  
■Advanced Films  
■PGS Graphite Sheet  
■Shield Film

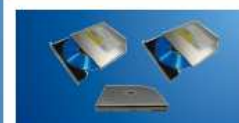


## 半導体

Semiconductors  
半導体



■マイクロコンピュータ  
■画像撮像素子  
■専用IC  
■センサ  
■GaAsデバイス  
■トランジスタ  
■統合デバイス  
■ダイオード  
■光半導体  
■ソリッドステートデバイス  
■ハイブリッドIC  
■Microcomputers  
■Image Pickup Devices  
■Application-Specific  
■Standard-Product ICs  
■Sensors  
■GaAs/AlGaAs Devices  
■Transistors  
■Multi-Chip Diacrits Devices  
■Diodes  
■Opto Electronic Devices  
■Solid State Devices  
■Hybrid IC



## 記憶デバイス

Storages, Supplies  
記憶デバイス



■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  
工場自動化設備



■FAセンサ  
■レーザーマーカ  
■プログラマブルコントローラ  
■画像処理機器  
■プログラマブル表示器  
■ライトカーテン(安全センサ)  
■省エネ監視機器  
■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  
電源・電池・エネルギー機器



■電源ユニット  
■電源部品  
■リチウムイオン電池  
■ニッケル水素電池  
■鉛酸電池  
■リチウム  
■マイクロナンテリ  
■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  
モータ、風扇、圧縮機



■FA用産業用モータ  
■家電用・産業用モータ  
■冷却デバイス  
■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各社で開発・製造。 Developed and manufactured within other Panasonic group companies.

# デバイスへのニーズとシーズ



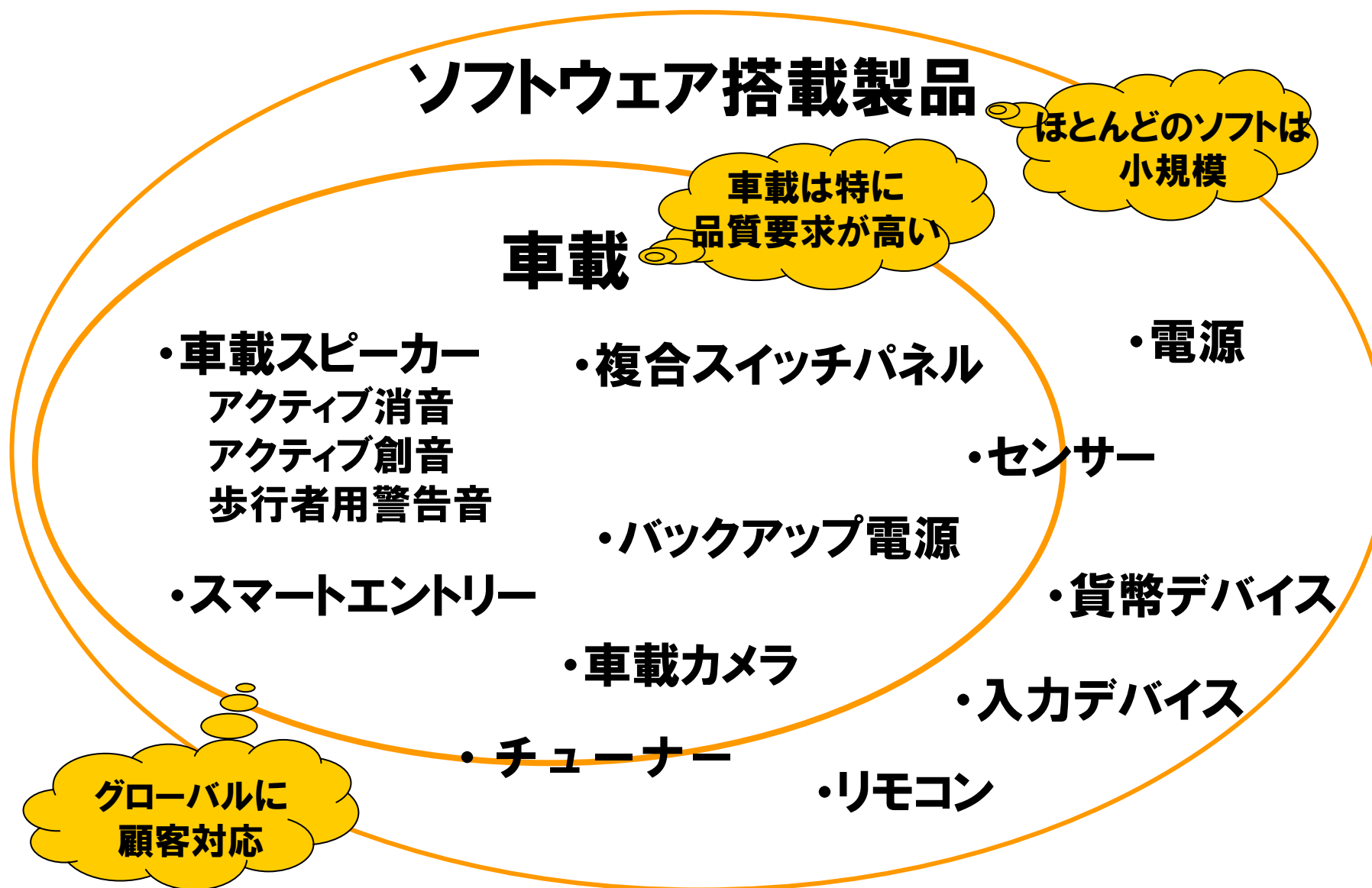


# グローバル拠点



**Panasonic** ideas for life

# デバイス社のソフトウェア搭載製品

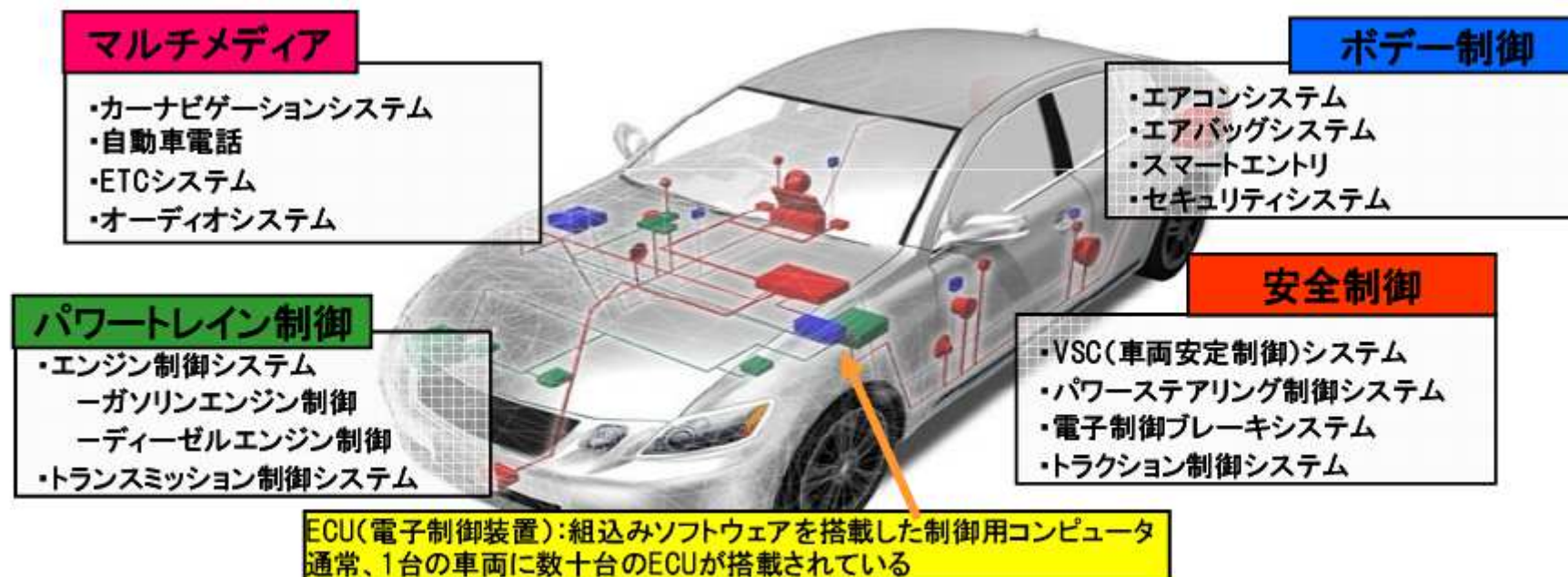


# 自動車の機能安全

- 車載システム
- 安全規格の体系
- 安全を脅かす原因と機能安全



# 車載システム



経済産業省「組込みソフトウェア産業活性化プラン」より転記

車載システムは、信頼性が高く、安全が要求されているが

- ・ECUが増加している
- ・電子制御への依存性がますます高まっている
- ・ソフトウェアの大規模化、複雑化
- ・多機種、複数機種並行開発
- ・厳しい性能要求

# 安全規格の体系

## ISO/IEC Guide51

Safety aspects – guidelines for  
their inclusion in standards

1990年代

### タイプA規格

(基本安全規格)  
すべての機械類に適用でき  
る基本概念、設計原則及び  
一般的側面を規定する規格

ISO12100 (基本概念)  
ISO14121 (リスクアセスメント)

2000年代

### タイプB規格

(グループ安全規格)  
広域な機械類に適用できる安全面  
または安全防護策を規定する規格

ISO13849 (システム安全)  
**IEC61508 (E/E/PE機能安全)**  
IEC60204 (電気設備安全)  
IEC62046 (人センシング)  
IEC61491 (産業機械の電気装置)

2010年代

### タイプC規格

(個別機械安全規格)  
個々の機械または機械群の詳細  
な安全要求事項を規定する規格

IEC61511 (プロセス産業)  
IEC61800 (電子制御モータ)  
IEC62304 (医療機器)  
IEC62061 (産業機器)  
ISO10218 (ロボット)  
**ISO26262 (自動車の機能安全)**

**Panasonic** ideas for life

# 本質安全と機能安全

**安全：受容できないリスクがないこと**

**本質安全：ハザード(危険源)を排除あるいは隔離して得られる安全**

**機能安全：安全装置を用いてリスクを軽減することで許容される安全**

＜例＞鉄道の踏切事故

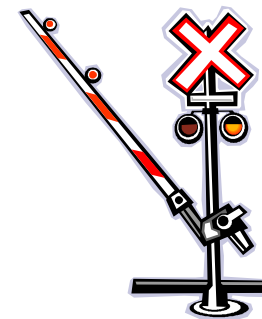
## 本質安全

鉄道の踏切をなくして  
すべて立体交差にすれば  
踏切事故はなくなる



## 機能安全

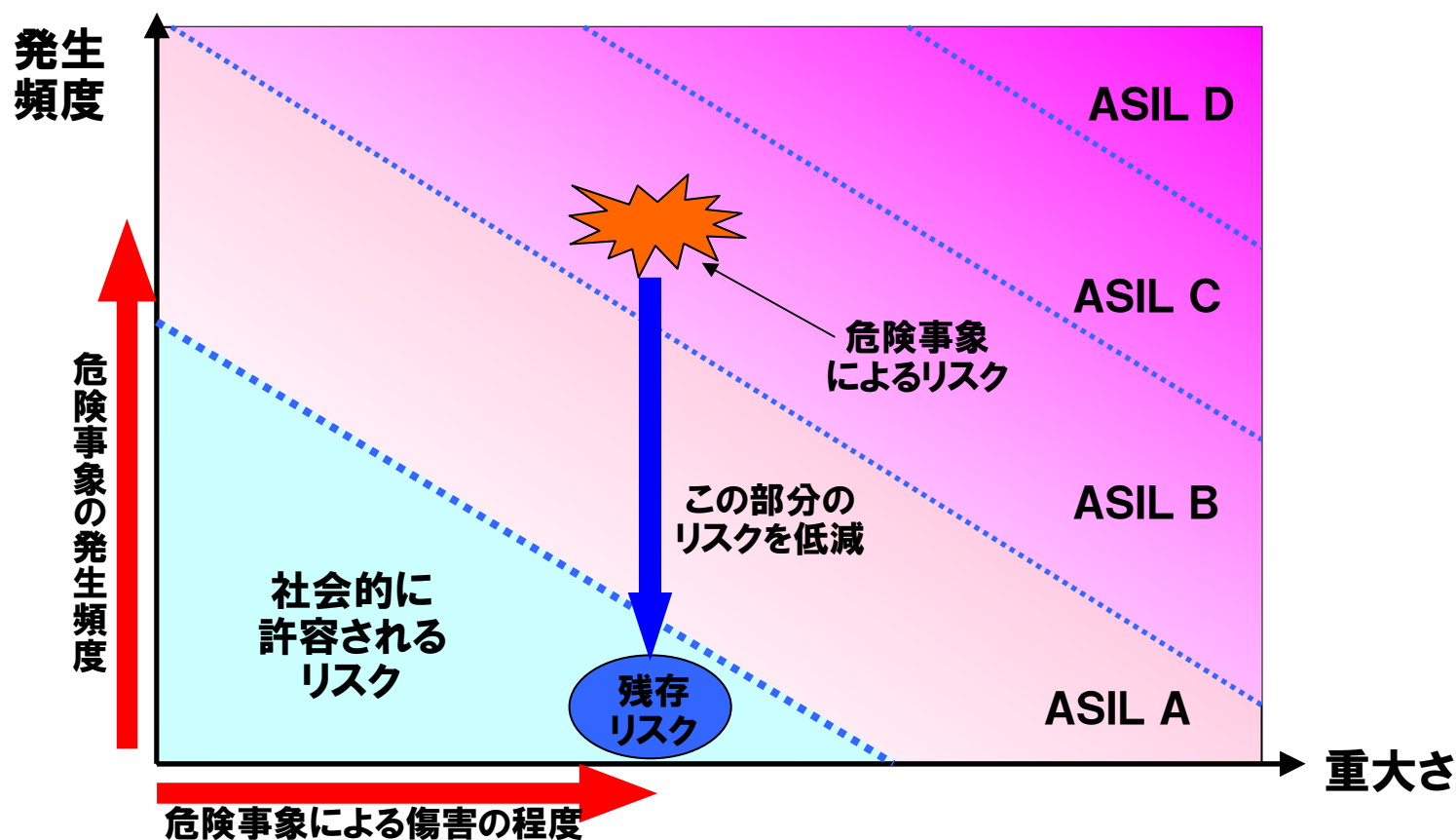
警報機、遮断機などの  
「安全装置」をつけて  
踏切での一定の安全を確保する



# リスク低減の考え方

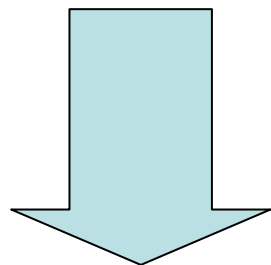
- 本来のリスクを、社会的に許容可能な水準に低減する
  - そのために、設計上の工夫、安全装置の付加などを行う

ASIL : Automotive Safety Integrity Level



# 安全を脅かす原因と機能安全

## 安全を脅かす原因



## 故障

### 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

例えば

- ・作業従事者の知識、技術不足により不具合が入る
- ・仕様や設計漏れ
- ・組織間の要求事項の漏れ

ソフトウェアやハードウェア(回路)設計

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

### 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に発生する故障

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

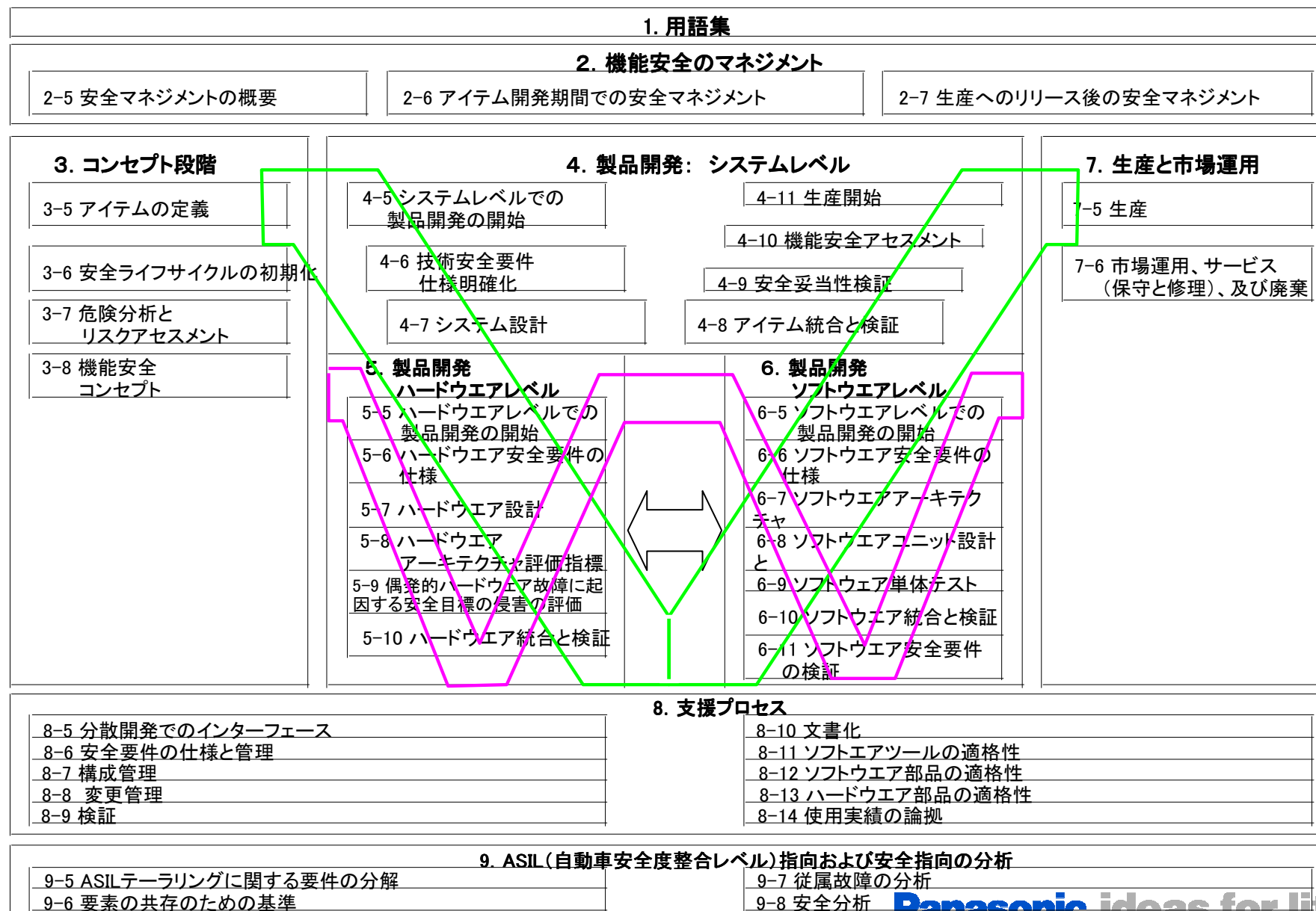
機能安全規格では、上記故障を発生させないため、安全プロセスや安全設計が規定されている

# ISO26262の要求

- ISO26262の構成
- ISO26262の要求例



# 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	確証対象	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	<ul style="list-style-type: none"> <li>・安全計画に計画された成果物</li> <li>・機能安全プロセスの実施</li> <li>・安全方策の適切性, 効率性</li> </ul>	審査

# ソフトウェア設計への要求例

## ソフトウェアアーキテクチャ設計の原則

手法	ASIL				
	A	B	C	D	
コンポーネントの階層構造	++	++	++	++	強く推奨
コンポーネントの規模制限	++	++	++	++	
インターフェース数の制限	+	+	+	+	推奨
コンポーネントの高凝集度	+	++	++	++	
コンポーネントの低結合度	+	++	++	++	
適切なスケジューリング属性	++	++	++	++	
制限された割り込みの仕様	+	+	+	++	

## ソフトウェアアーキテクチャレベルのエラーハンドリングのメカニズム

手法	ASIL			
	A	B	C	D
静的リカバリーメカニズム	+	+	+	+
グレースフルデグラデーション	+	+	++	++
独立した並列冗長	0	0	+	++
データのための修正コード	+	+	+	+

 **ソフトウェア設計プロセスに埋め込み**

# ハードウェア設計への要求例

- 以下の両方を満たすように設計する

## I. ハードウェアアーキテクチャの評価

- SPFM(単一フォールト)
- LFM(潜在フォールト)

SPFM

ASIL B	ASIL C	ASIL D
>90%	>97%	>99%

LFM

ASIL B	ASIL C	ASIL D
>60%	>80%	>90%

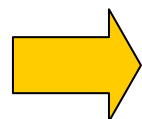
## II. ランダムハードウェア故障に対するリスクの評価

- PMHF(目標違反の最大確率に対する定量的目標値)  
...参照値を利用して設定

### ➤ システムアーキテクチャが、

- ランダムハードウェア故障の対処に効果があること、
- ランダムハードウェア故障の発生確率が抑えられていること

の両方の論理的な根拠が必要



**ハードウェア設計プロセスに埋め込み**

# 確証方策の第三者性への要求例

確証方策には、確証レビュー、機能安全監査、機能安全アセスメントがある

確証方策	ASIL			
	A	B	C	D
ISO26262に準拠して扱われるアイテムのハザード分析とリスクアセスメントの確証レビュー (アイテムの開発者から独立)	I3			
安全計画の確証レビュー (アイテムの開発者、プロジェクトマネジメントから独立)	-	I1	I2	I3
統合とテスト計画の確証レビュー (アイテムの開発者、プロジェクトマネジメントから独立)	I0	I1	I2	I2
妥当性確認計画の確証レビュー (アイテムの開発者、プロジェクトマネジメントから独立)	I0	I1	I2	I2
安全解析(FMEA、FTA)の確証レビュー	I1	I1	I2	I3
ソフトウェアツールの確証レビュー (ソフトウェアツールの認定者から独立)	-	I0	I1	I1
ASIL候補の根拠(分析、データ、信頼度)の確証レビュー (根拠の供給者からの独立)	I0	I1	I2	I3
安全ケースの完全性の確証レビュー (安全ケースの提供者から独立)	I0	I1	I2	I3
機能安全プロセスの監査 (機能安全に要求されるプロセスに準じて作業する要員から独立)	-	I0	I2	I3
機能安全アセスメント (安全ケースの提供者から独立)	-	I0	I2	I3

監査

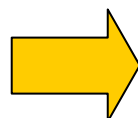
審査

I0: 確証方策を実施したほうがよい(Should)

I1: 確証方策が実施しなければならない(Shall)

I2: 確証方策が別のチームの要員によって実施されること(例: 同じ直属の上長に報告しない)

I3: 確証方策が別の部署、組織の要員によって実施されること



レビュー、監査、審査プロセスに埋め込み

Panasonic ideas for life

# デバイス社のシステムプロセス監査

- システム製品開発プロセスのB/A
- デバイス社システム製品の開発フェーズとイベント(システム製品開発管理規程)
- プロセス監査
- SQAのスキルマネジメント

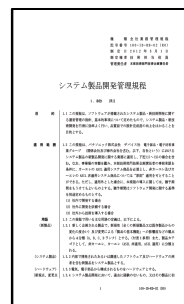


# システム製品開発プロセス

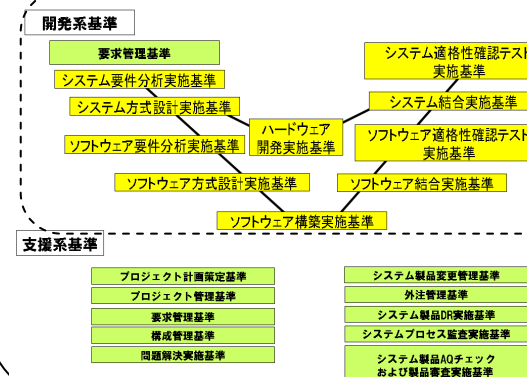
★機能安全  
★短納期化  
★複雑化

対応

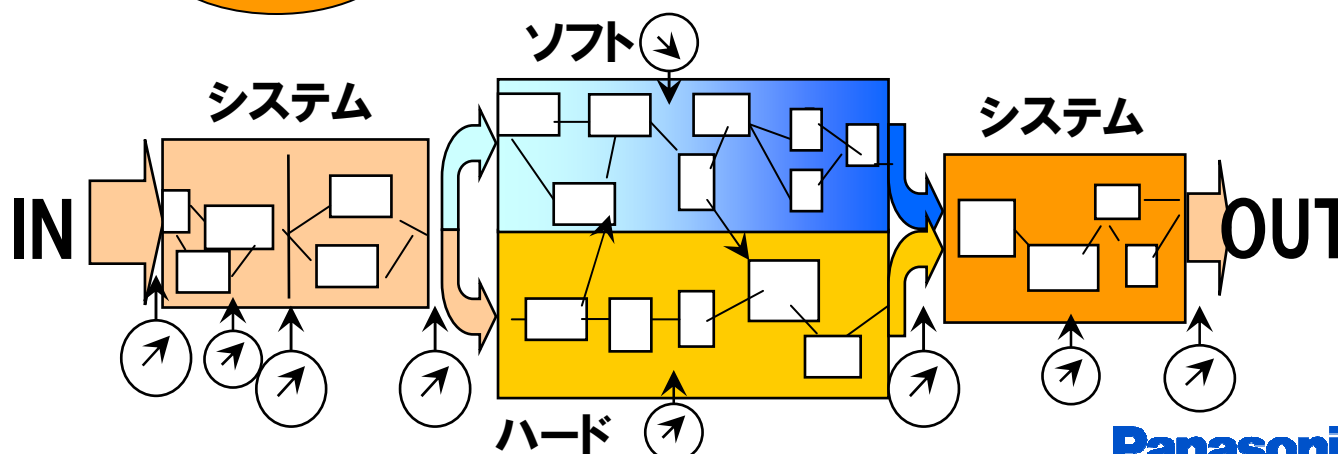
システム製品開発管理規程、  
関連実施基準、  
ガイドライン、  
テンプレート、  
チェックリスト



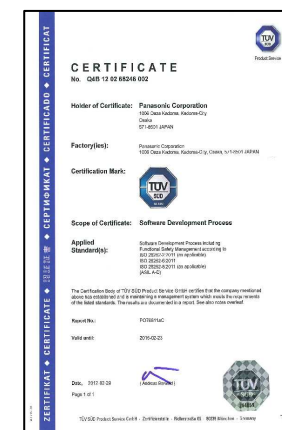
## プロセスの構成



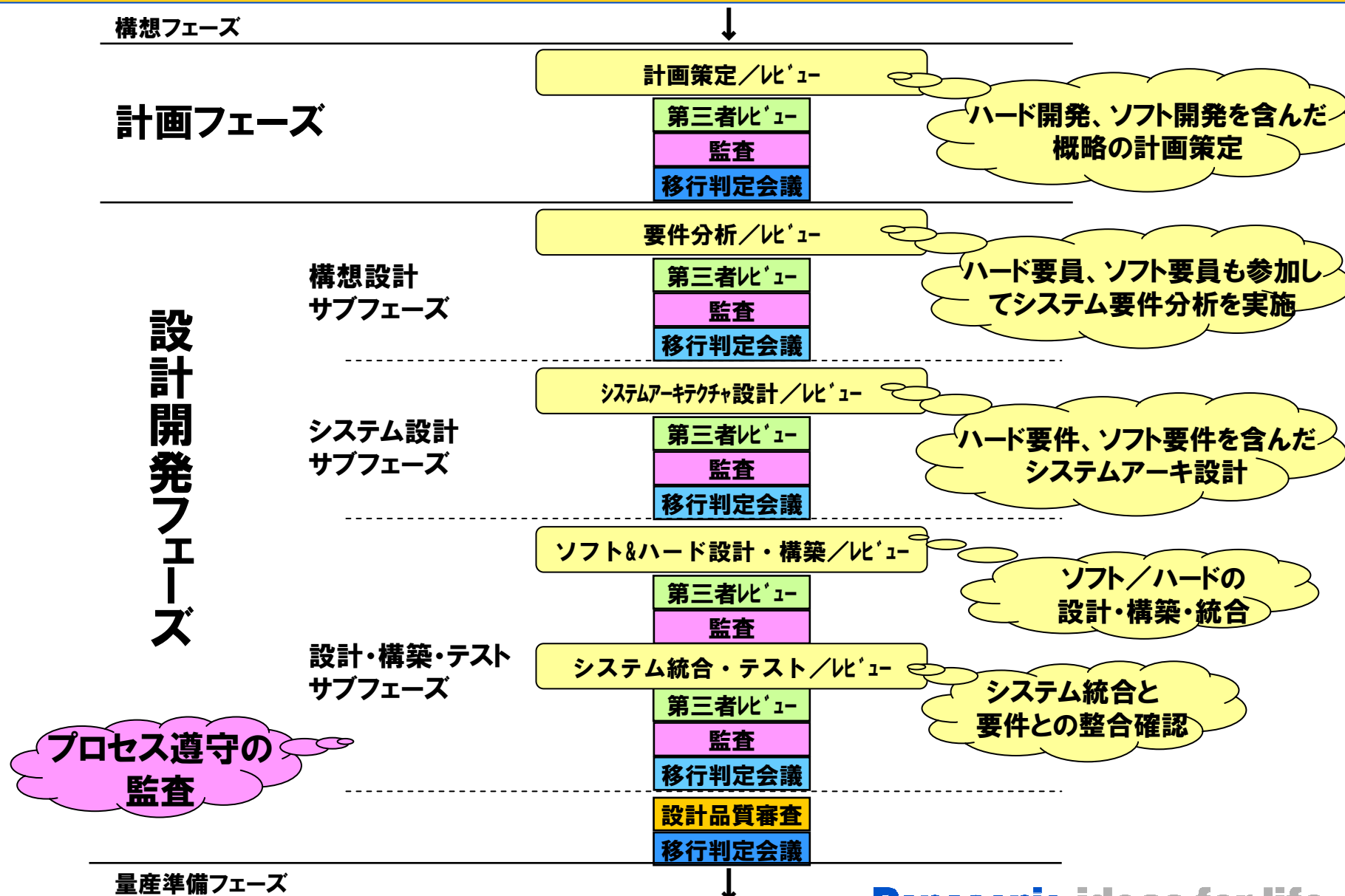
- ・機能安全要求実施
- ・SYS/HW/SW整合強化
- ・エビデンス強化



## プロセス認証



# デバイス社システム製品の開発フェーズとイベント



# 監査活動

## 監査対象プロセスの選択 (プロジェクト開始時)

必要に応じ、  
ハードウェアも監査対象とする

システム System		ソフトウェア Software		ハードウェア/量産関連 Hardware/Product		支援プロセス Support	
A	要件管理 Requirement Management	A	要件分析 Requirement Analysis	NA	ハードウェア設計 HW Design	A	外注管理 Subcontractor Management
A	要件分析 Requirement Analysis	A	方式設計 Architecture Design	NA	ハードウェア構築、テスト HW Construction & Test	A	構成管理 Configuration Management
A	方式設計 Architecture Design	A	構築 Construction	NA	6.13 生産準備 Production Preparation	A	ベースラインの作成と監査 Baseline audits
A	結合 Integration test	A	結合 Integration test	A	7. 量産試作品のテスト SYOT for Mass Production	A	問題解決管理、変更管理 PR,CHM
A	適格性確認テスト Qualification Test	A	適格性確認テスト Qualification Test	A	8. プロジェクトの完了 Completion of Project	A	計画、進捗管理 PP,PM

監査対象活動  
を選択

A B C			F G H			J K L			M			N O P			R S T			U			V W X			Y			AG AE AF AG		
プロジェクト(Project) 1			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 2			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 3			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 4			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 5			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 6			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 7			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 8			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 9			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 10			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 11			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 12			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 13			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 14			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 15			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 16			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 17			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 18			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 19			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 20			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 21			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 22			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 23			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 24			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 25			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 26			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 27			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 28			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 29			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 30			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 31			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 32			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 33			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 34			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 35			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 36			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 37			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 38			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 39			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 40			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 41			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 42			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 43			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 44			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 45			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 46			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 47			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 48			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 49			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 50			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 51			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 52			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 53			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 54			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 55			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 56			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 57			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 58			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 59			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 60			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 61			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 62			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 63			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 64			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 65			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 66			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 67			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 68			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 69			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 70			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 71			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 72			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 73			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 74			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 75			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 76			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 77			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 78			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 79			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 80			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 81			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 82			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 83			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 84			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 85			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 86			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 87			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 88			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 89			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 90			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 91			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 92			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 93			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 94			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 95			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 96			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 97			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 98			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 99			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 100			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 101			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 102			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 103			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 104			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 105			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 106			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 107			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 108			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 109			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 110			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 111			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 112			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 113			SQS			SQ0			SQ1			SQ2			SQ3			SQ4			SQ5			SQ6			SQ7		
プロジェクト(Project) 114			SQS			SQ0			SQ1			SQ2			SQ3														

# チェックリスト

4.3 プロジェクト管理	A				A				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 SQS												
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 SQO												
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 システム適格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 SQ1												
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 ソフトウェア実装とテスト												
6.16.1 ソフトウェア構築(詳細設計)	A											
6.16.1 ソフトウェア構築(実装・静的解析)	A											
6.16.1 ソフトウェア構築(単体テスト)	A											
6.16.2 ソフトウェア構築レビュー	A											

**6.10 ソフトウェア設計-6.10.4 ソフトウェア設計**

<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」SWRAを実施。又は、システムアーキテクチャ設計書でソフトウェア要件を確認する(SWAD3.1.1)
- 2)「コンポーネント分割」
- 3)「インターフェース設計」
- 4)「静的構造/動的構
- 5)「機能の設計」コン
- 6)「一貫性・正確性確
- 7)「データ構造の設計
- 8)「見積り」コンポーネ
- 9)「影響範囲確認」
- 10)「文書化」SWADの結果をまとめて、「ソフトウェアアーキテクチャ設計書」を作成(改訂)する(SWAD3.1.3)

<プロセス実施の観点>

- 1)要件に関
- 1)必要な開
- 2)ソフトウェア
- 2)「新規/流
- 2)必要に応じて、設計基準を参照し、複数のソフトウェアアーキテクチャの候補の中から最適なものを決定する(SWAD3.1.2)

<機能安全の観点>

ソフトウェア  
ソフトウェア  
ソフトウェア  
ソフトウェア  
ソフトウェア

**機能安全の観点**

カニズ

<コメント>

save

# 機能安全のチェック項目

技術側でのレビューで確認後、SQAによる抜き取りでの確認を想定

要求事項はASILにより異なる

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				作業成果物 work products
				A	B	C	D	
(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。	具体的な 確認事項：  テンプレートの 該当項目など	++	++	++	++	安全コンセプト仕様書 functional safety concept 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。		++	++	++	++	安全コンセプト仕様書 functional safety concept 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されなければならない。		-	-	-	-	安全コンセプト仕様書 functional safety concept 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		++	++	++	++	
		5 e) 機能冗長性		++	++	++	++	
	FS3-8.4.2.4	1 もし、受容可能な時間間隔に、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。		++	++	++	++	安全コンセプト仕様書 functional safety concept 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。		++	++	++	++	安全コンセプト仕様書 functional safety concept specification
	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ついて作成されるなら、：		-	-	-	-	安全コンセプト仕様書 functional safety concept specification
		1 a) これらの行動は、機能安全コンセプトに特定されなければならない。		++	++	++	++	
		2 b) 運転者もしくは他の危険に晒される可能性のある人についての適切な手段ならびに制御は、機能安全コンセプトの中で特定されなければならない。		++	++	++	++	

# SQAのスキルマネジメント

## 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③)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項目に關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こみ、改善ができる。		5以上のレベルを有する者で、学会や研修会等で当社の活動を発表できる。									
	PEDソフト協業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監査活動の監査への参加経験有り。(監査メンバー)		★PED内SQA監査活動の監査実施経験有り。											
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		★PASSPORTアセスメント以上の資格を有する		★PASSPORTリードアセスメントの資格を有する												
トレーニングマップ	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			レベル4までに受講			レベル5までに受講			レベル6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	研修名(開催組織)			計画	実績
	品質保証/品質管理全般	★PEF賞																			
	ソフトウェア品質保証(SQA)																				
	エンジニアリング/安全																				
	ソフトウェア(システム)開発プロセス																				
	PEDソフトウェア開発プロセス																				
	★SQA監査(DQC)						★SQA監査(DQC)チェックリスト(DQC)														



# まとめ

- 車載のシステム製品開発において、機能安全要求を満たせるシステム、ハード、ソフトの開発プロセスを定義した。
- 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した。
- 今後の取り組み予定
  - ・監査員の更なるレベルアップ（ノウハウ蓄積と展開）
  - ・機能安全監査、伊能安全審査、第三者レビューの連携強化
  - ・システム製品開発プロセスの改善（SEPGと連携）

ご清聴ありがとうございました

**Panasonic**  
ideas for life

