自動車の機能安全と部品安全
～ISO 26262の概要～

2015/10/21

パナソニック(株)
オートモーティブ＆インダストリアルシステムズ社
技術本部　プラットフォーム技術開発センター
システム技術開発部　機能安全推進課
安倍秀二

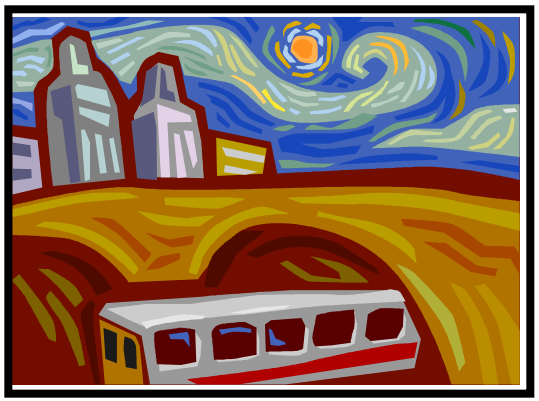
JEITA

機能安全規格とその要求

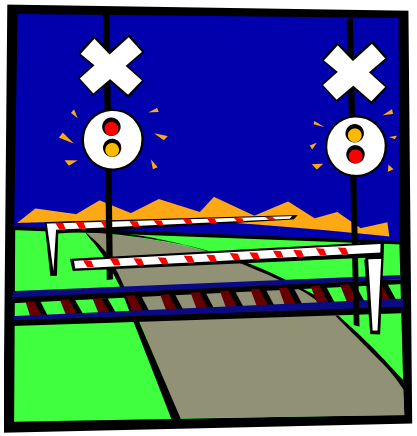
本質安全と機能安全

- 本質安全とは、
  - 機械が人間や環境に危害を及ぼす原因そのものを低減、あるいは除去する
- 機能安全とは、
  - 機能的な工夫（安全を確保する機能：以下、安全機能）を導入して、許容できるレベルの安全を確保すること
    - 安全機能を実行する主体を安全関連系と呼ぶ
    - ハードウェアだけではなく、ソフトウェアも対象に入る(ECU)

立体交差

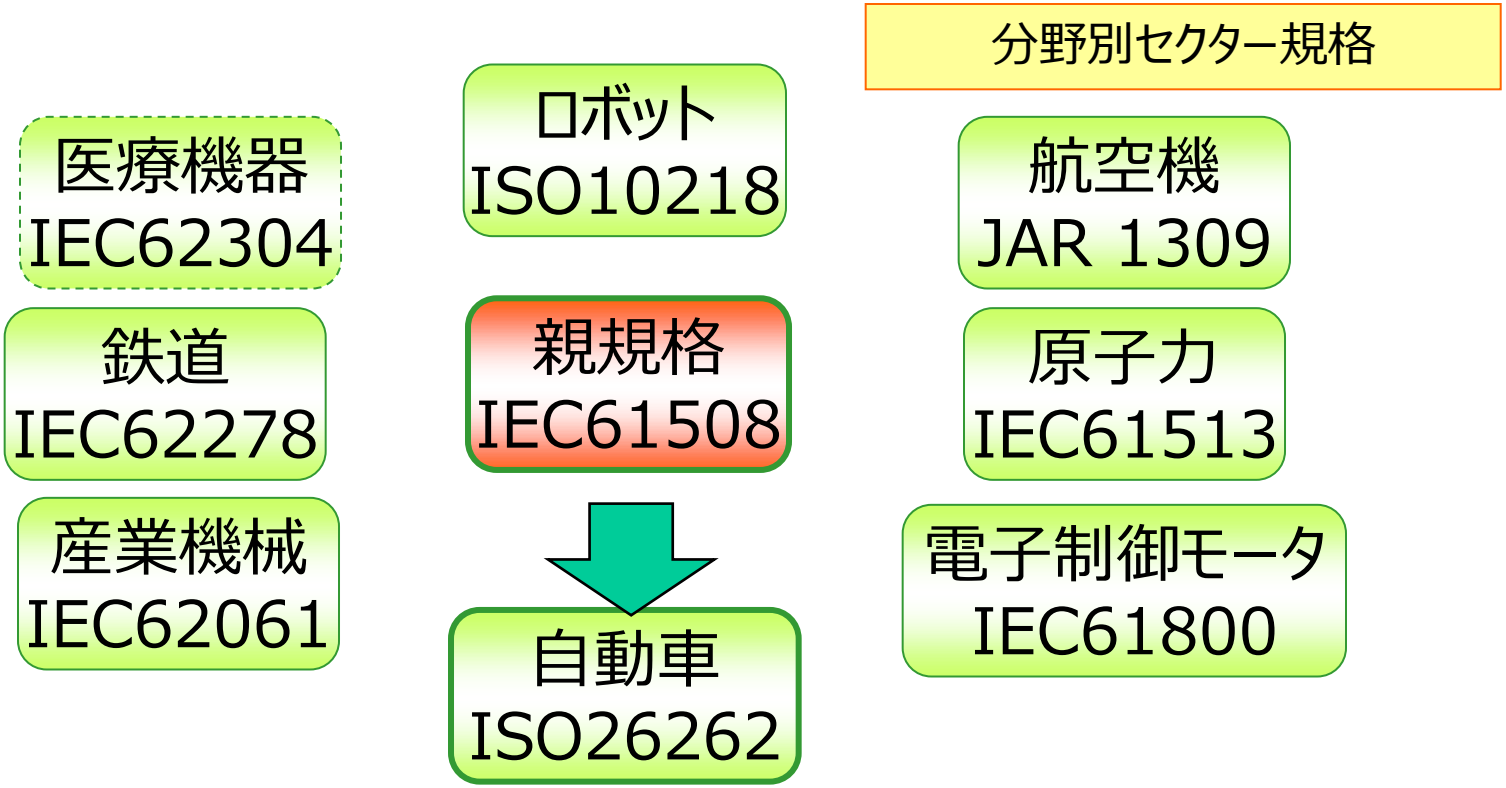


踏切



機能安全規格群

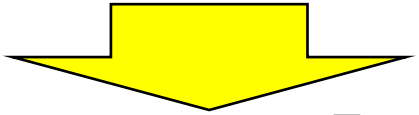
親規格であるIEC61508は、プラントを中心とした電気電子機器の機能安全規格　⇒　分野ごとの特性に応じ派生



2011年に制定。国内外のカーメーカから、規格を遵守したシステム開発が求められる。
サプライヤは、機能安全に対する備えが必要。

ISO 26262規格制定の背景

- 自動車の電子化による機能のブラックボックス化
- ECU間の連携動作や複数サプライヤ開発による複雑化
- 事故で発生した人的被害・物的損害に対し、誰かが‘責任’を取らなければならない
- 最終的に裁判所で‘責任’が決定される

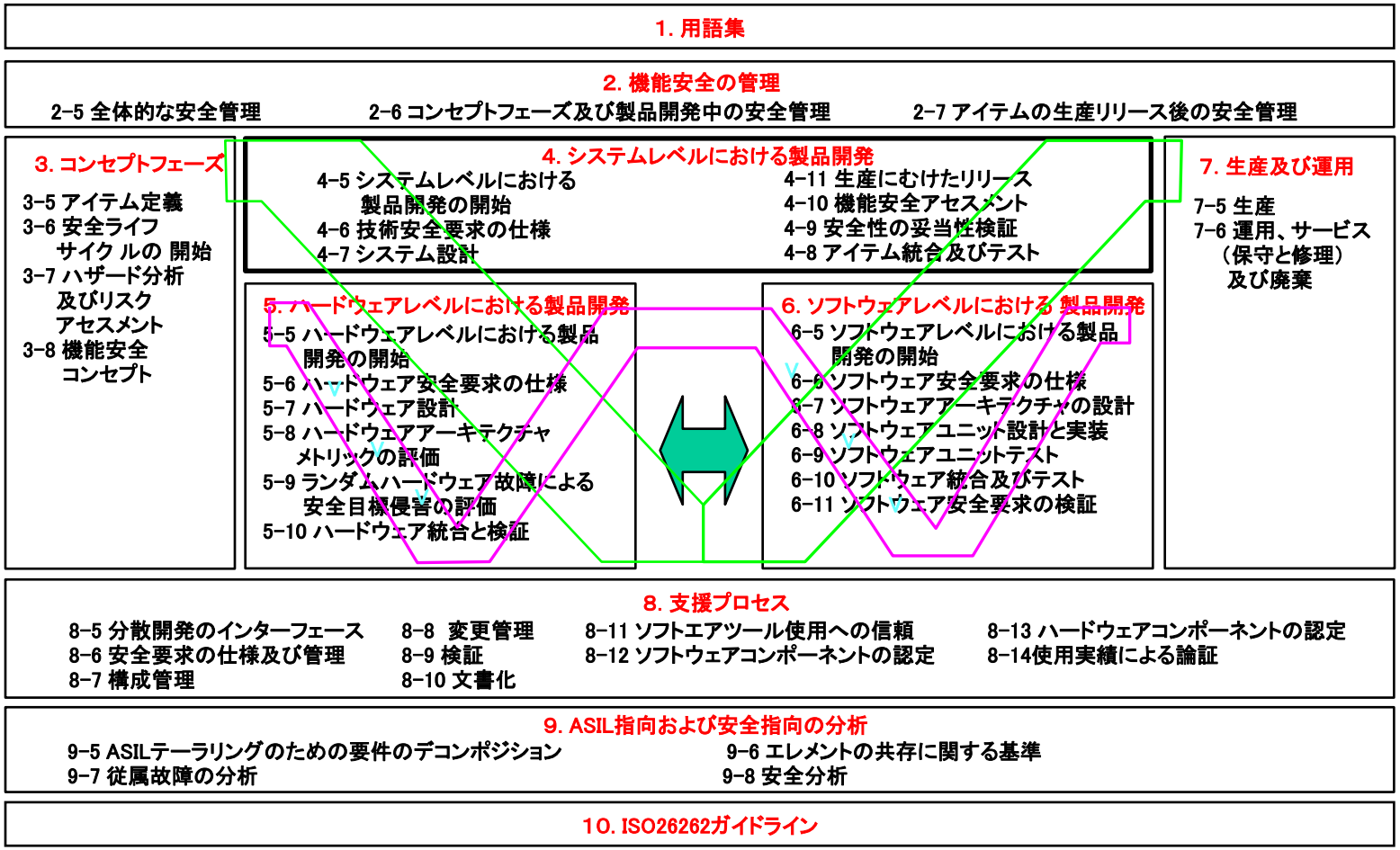


- 「機能安全」の考え方により、『被害０』を目指す
- 安全性を軸に開発業務全体を見える化し、説明責任を果たすとともに、訴訟に耐え得る証拠を揃える

ECU: Electric Control Unit

ISO 26262規格の構成

自動車の組込み電気/電子/PEシステムの開発ライフサイクルを規定
システム、ソフト、ハードの各開発段階で、V字モデルを定義



「機能安全規格　ISO 26262:2011　より引用」

ISO 26262規格の適用範囲

- 車両総重量が最大3.500kgまでの量産される乗用車に組み込まれる、安全関連システム
- **E/E（電気/電子）**安全関連システムの**機能不全のふるまい**によって引き起こされる可能性のある潜在的なハザードを取り扱う
- 感電、火災、発煙、熱、放射線、毒性、可燃性、反応性、腐食、エネルギーの放出および同様のハザードに関連するハザードは、E/E安全関連システムの機能不全のふるまいが直接の原因でない限り取り扱わない
- 機械系は、“アザーテクノロジー”として位置づけ、適用外
  - E/E関連機器に設定された機能安全要求をアザ-テクノロジーに配置することで、ISO 26262の適用外になる

「機能安全規格　ISO 26262:2011　より引用」

ハザードとリスク

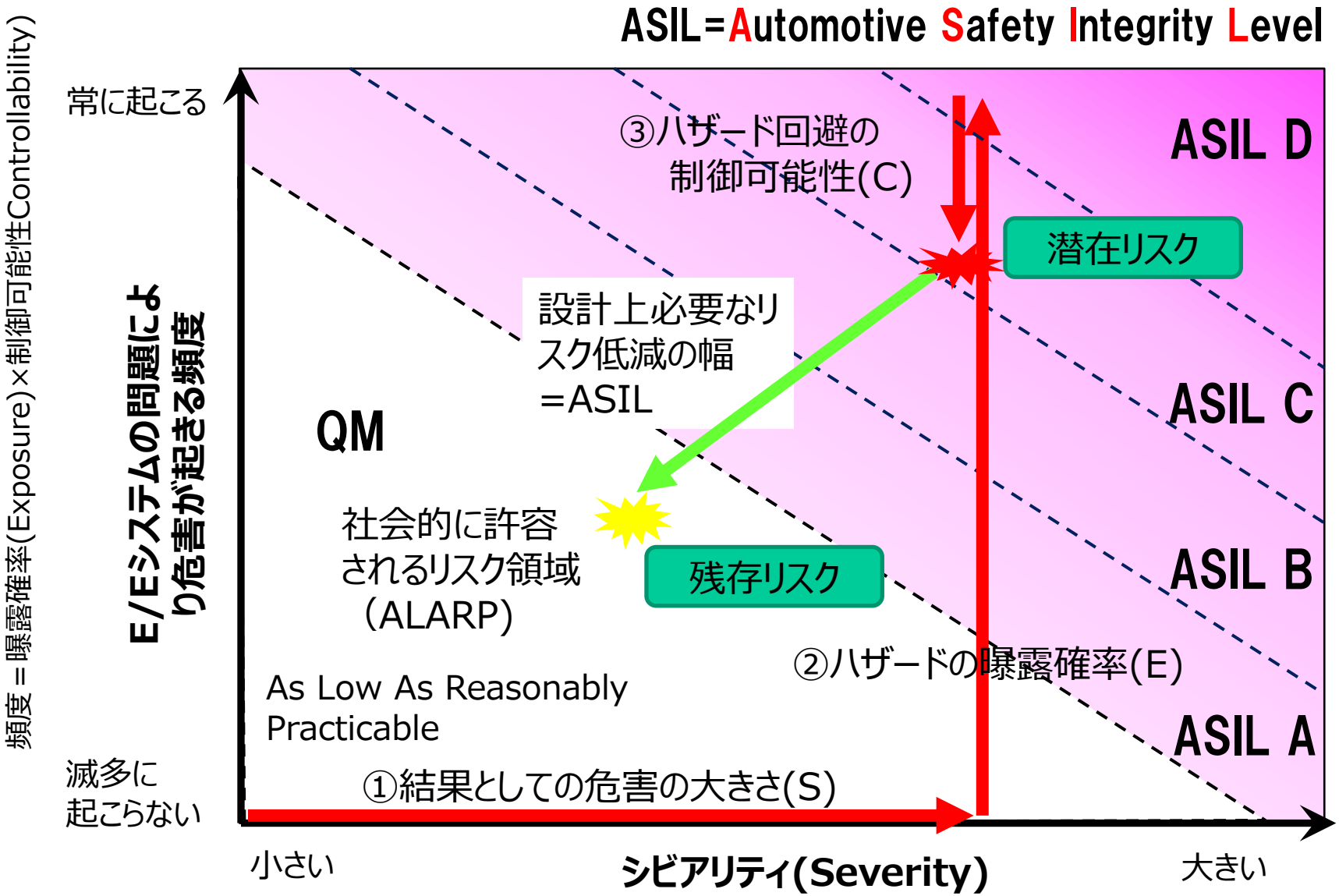
(例)作業場所にある電気が流れている裸電線

- ハザード（Hazard）
  - 怪我や物理的なダメージを生じる可能性のある原因（ソース）
    - (例)電気が流れている100Vの裸電線
- 危険事象（Hazardous event）
  - ハザードと運用状況が組み合わさったもの
    - 裸電線に素肌の腕が触れる
- リスク（Risk）
  - 危害発生の可能性とその重大さの組合わせ
    - 100Vに腕が接触した場合の傷害の程度（シビアリティ）と素肌の腕が触れる可能性の積

自動車の場合

自動車に内蔵されているECUの問題(ハザード)により、自動車の機能が損なわれる(機能不全)潜在リスクを取り扱う

自動車の機能安全でのリスク低減の考え方

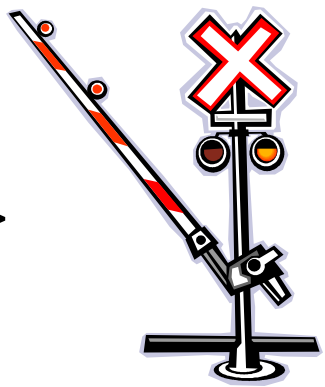


出展：日経エレクトロニクス　2011.1.11(改変)

リスク低減のために

- 安全に対するリスクに応じて安全度合を決定し、必要な安全機能（方策）を選択する
  - 安全度合は、安全に動作する程度
  - 安全機能は、リスクを許容できる水準まで低減するための機能

<対策例>



街中の道路
電車本数多い
見通しが悪い

>

>

田舎道
電車本数少ない
見通しが良い

ISO26262が要求する内容

- 開発・管理活動を体系的に実施し、客観的に検証が可能な証跡を残す、仕組みを構築
  - 安全ライフサイクルによる安全計画の策定
  - 設計の根拠の提示
  - 検証活動の徹底
  - 確証方策による安全活動の客観的検証
  - 安全ケースによる安全論拠の提示
- 機能安全プロセスの定義と遵守
  - 規格要求内容を含んだ機能安全プロセスの定義
  - 機能安全プロセスを遵守し、人的ミスの入らない開発
  - 十分信頼の高い設計などの再利用
- 設計ミスを起こさない開発と市場で発生する可能性のある機能安全に対するフェールセーフ

機能安全と品質

品質
信頼性

故障してはいけない

高信頼設計
高信頼部品

機能安全

故障は起こるもの

故障に対するリスクの備え

ともに満たすことが必要

ISO26262の基盤

How

ISO26262

What

業界モデル

TS16949	VDA6.3	Automotive SPICE	CMMI Dev
自動車業界向け QMS規格	ドイツ 自動車工業規格	車載SW開発の プロセスモデル	開発のプロセス改善 に役立つ プロセスモデル

汎用モデル

ISO9001（QMS）
品質マネジメントシステムに関する規格

概念

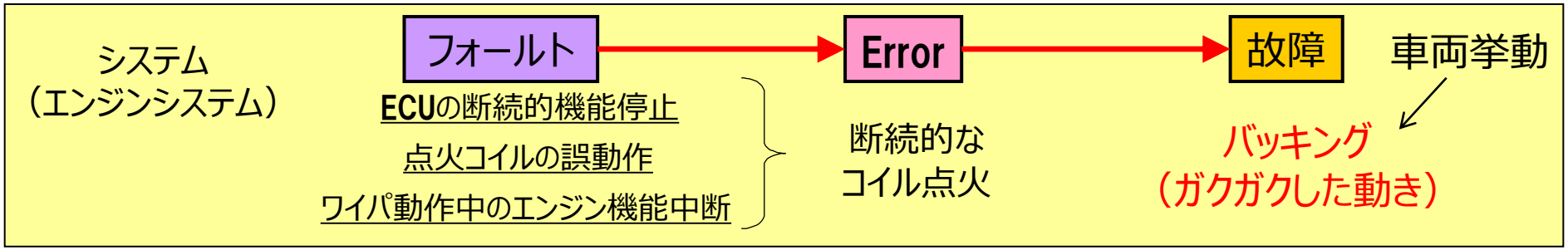
プロセスアプローチ、継続的改善（PDCA）

JEITA

機能不全とその原因

故障、エラー、フォールト

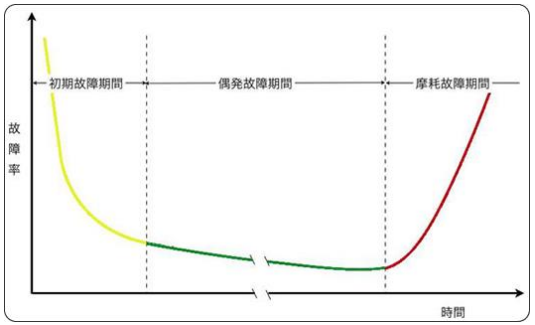
- 故障 （Failure）
  - 要求された機能を実行するシステム(ECU)の能力の停止
- エラー （Error、誤り）
  - 計算，観測又は測定された値あるいは条件と，実際の指定された又は理論的に正しい値あるいは条件との不一致
- フォールト（Fault）
  - システムあるいは車両の故障を引き起こす可能性のある，異常な状態



「機能安全規格　ISO 26262:2011　より引用」

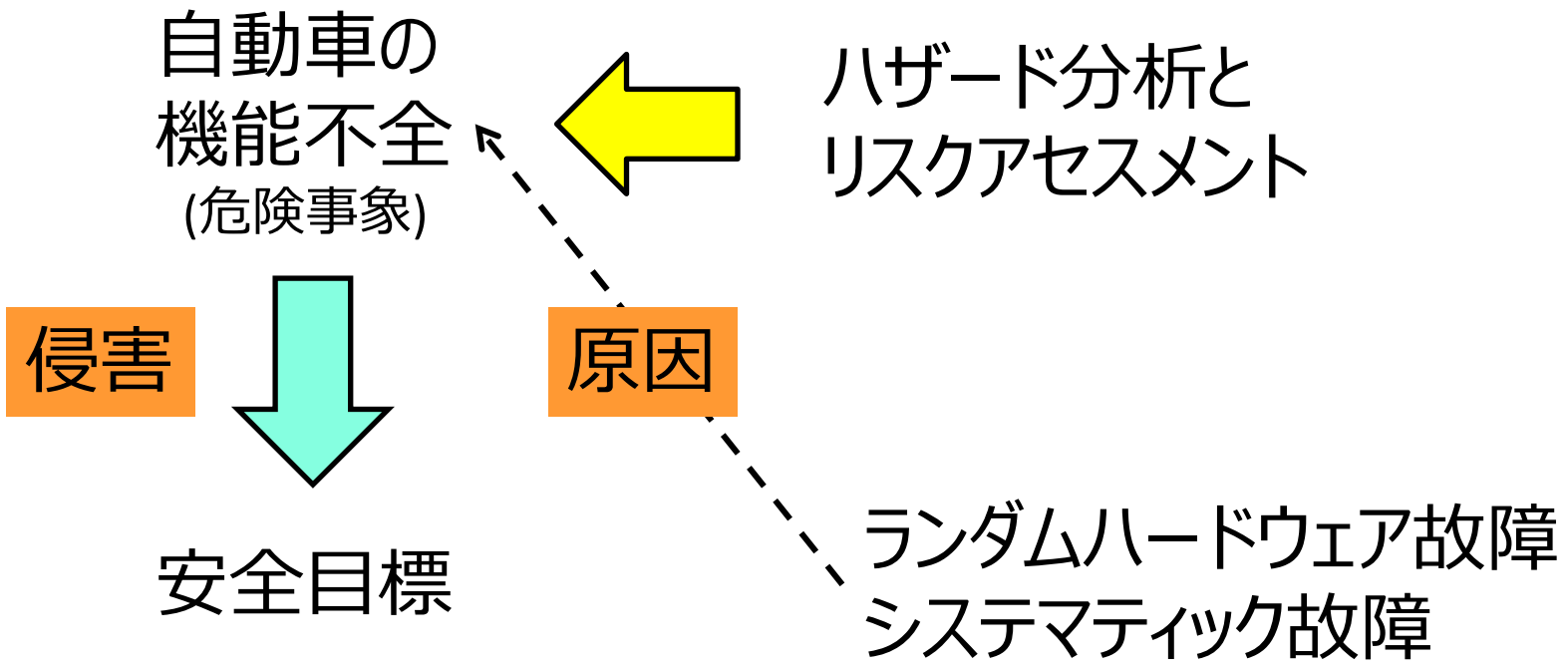
ISO 26262が取り扱う機能不全を引き起こす故障の種類

- ランダムハードウェア故障
  - ハードウェア部品の故障についての確率分布に従い発生し、発生する時を予期できない故障



- システマティック故障
  - 決定論的に発生する故障

機能安全の基本的な考え方



- 機能安全を達成すること(故障が起こっても、安全目標を侵害しない)
- 機能安全の達成が説明できること（安全ケース）

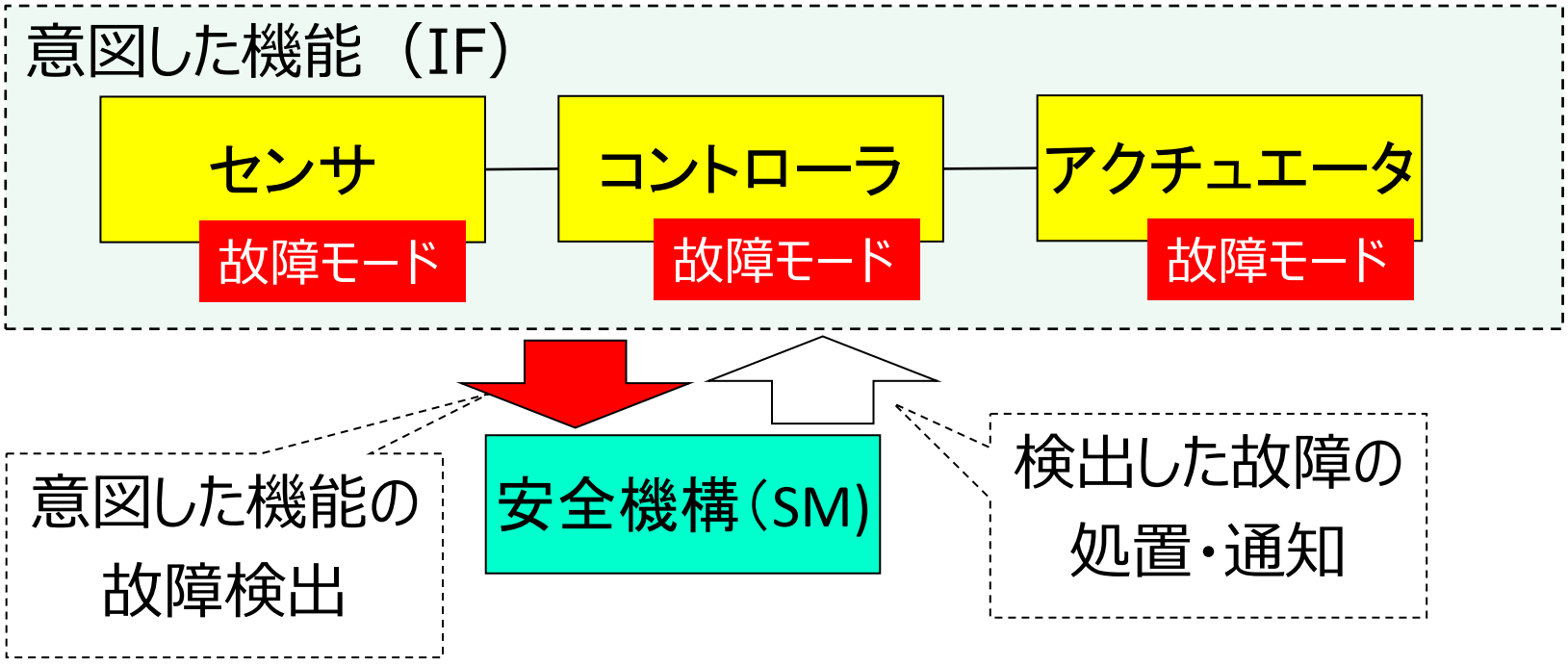
故障の原因と対策

- ランダムハードウェア故障
  - 原因
    - 電気部品の確率的に発生するフォールト
  - 対策
    - 出荷後に起きることを想定
    - フォールトの検出と緩和の方策により、リスクを減らす

- システマティック故障
  - 原因
    - 設計ミス、実装ミス、製造ミスなどのヒューマンエラー
  - 対策
    - 出荷前に対策する
    - プロセス又は設計方策の適用によって防止

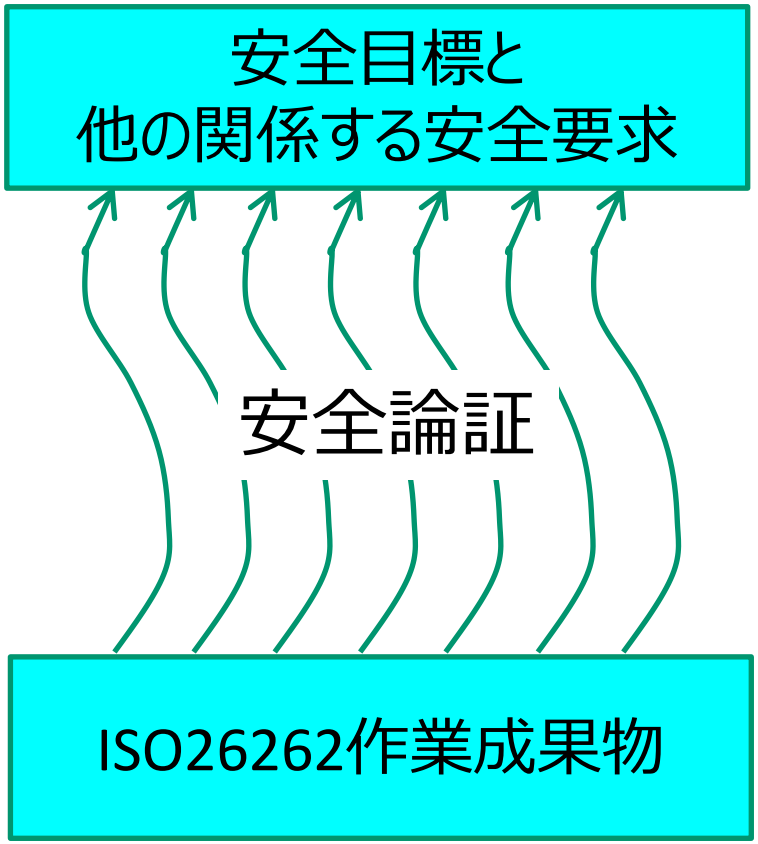
機能安全実現の基本戦略

- 電気/電子部品のフォールトを検出して処置し、安全状態を維持し、安全状態に遷移する
- 従来のフェールセーフの考え方の発展



安全ケース

システムが許容可能な程度に安全であることの正当性を主張するための構造化された論証



- 安全に関わる要求
  - 機能安全要求
    - 故障による安全目標違反の防止
- 安全に関わる要求の達成の論述
  - 安全に関わる要求と作業成果物をヒモ付ける
- 作業成果物
  - 論拠を裏付ける証拠としての実績

機能安全開発の備えと導入

開発フェーズ	開発の備え	実開発
開発前	● 機能安全プロセスの構築 ● 確証レビューの体制 ● スキル認定プログラムの確立	---
企画	---	● アイテムの定義 ● H&Rの実施 ● 機能安全コンセプトの立案
開発	---	● 安全管理者の任命 ● 安全計画の立案 ● 技術安全コンセプト ● システム設計 ● ハードウェア設計 ● ソフトウェア設計 ● 確証方策実施 ● 安全ケース
製造	● TS-16949あるいはVDA6.3要求の仕組み	● 安全関連特別特性の引き継ぎと実施

機能安全開発の組織の備え

- 機能安全プロセスの構築
  - ISO 26262、TS16949、AutomotiveSPICEをベースにしたプロセスの構築
- 機能安全の達成を客観的に評価
  - 確証方策(機能安全アセスメント、機能安全監査、確証レビュー)による客観的な評価
- 機能安全スキル強化とスキル認定
  - プロジェクトに配置する要員は、事前のスキル認定が必要

電気/電子部品のフォールトとハードウェア開発

車載開発の特徴と機能安全

調達側　　サプライヤ

サプライチェーンにより部品開発を分担

OEMやTierが部品を調達してシステムを組み立てる

調達先のサプライヤーに機能安全開発を要求

それぞれの部品の安全を確保するために機能安全開発を実践

システムレベルの安全の論証

DIA

- 作業成果物の範囲
- 開示・提出の取り決め

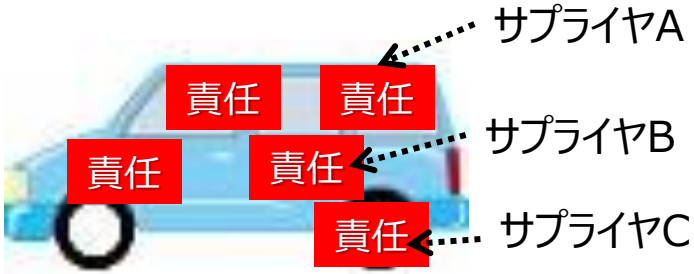
DIA:開発インタフェース協定

部品の安全への達成を証明する証拠をまとめる

安全ケース

サプライヤレベル安全ケース

説明



ハードウェア設計での考慮点

- ハードウェアレベルのアーキテクチャ設計
  - 電気/電子部品のフォールトの検出と対応
  - モジュール化、適切な粒度、単純性
    - 高凝集度、低結合度
- 詳細な回路設計
  - 故障率計算
    - 産業界データベースの利用(通常)
      - IEC62380、FIDES、SN29500
  - ハードウェアのアーキテクチャの評価のためのメトリクス目標(評価指標)の達成
    - SPFM and LFM
  - ランダムハードウェア故障の残存リスク評価
    - PMHF or メソッド2（カットセット法）

代表的な故障率データベース

TECHNICAL REPORT

IEC TR 62380

First edition
2004-08

Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment

IEC

Reference number
IEC/TR 62380:2004(E)

MATHEMATICAL MODEL :

$$\lambda = \left\{ \left[\lambda_1 \times N \times e^{-0.35\alpha} + \lambda_2 \right] \times \left[\sum_{i=1}^{y} \left(\pi_t \right)_i \times \tau_i \right] \right\}_{\lambda_{die}} + \left\{ 2.75 \times 10^{-3} \times \pi_\alpha \times \left[\sum_{i=1}^{z} \left(\pi_n \right)_i \times \left(\Delta T_j \right)^{0.68} \right] \times \lambda_3 \right\}_{\lambda_{package}} + \left\{ \pi_I \times \lambda_{EOS} \right\}_{\lambda_{overstress}} \times 10^{-9} / h$$

NECESSARY INFORMATION:

$(t_{ao})_i$: average outside ambient temperature surrounding the equipment, during the i^{th} phase of the mission profile.
$(t_{ac})_i$: average ambient temperature of the printed circuit board (PCB) near the components, where the temperature gradient is cancelled.
λ_1 : per transistor base failure rate of the integrated circuit family. See Table 16.
λ_2 : failure rate related to the technology mastering of the integrated circuit. See Table 16.
N : number of transistors of the integrated circuit.
a : [(year of manufacturing) – 1998].
$(\pi_t)_i$: i^{th} temperature factor related to the i^{th} junction temperature of the integrated circuit mission profile.
τ_i : i^{th} working time ratio of the integrated circuit for the i^{th} junction temperature of the mission profile.
τ_{on} : total working time ratio of the integrated circuit. With: $\tau_{on} = \sum_{i=1}^{y} \tau_i$
τ_{off} : time ratio for the integrated circuit being in storage (or dormant). With $\tau_{on} + \tau_{off} = 1$
π_α : influence factor related to the thermal expansion coefficients difference, between the mounting substrate and the package material.
$(\pi_n)_i$: i^{th} influence factor related to the annual cycles number of thermal variations seen by the package, with the amplitude ΔT_i .
ΔT_i : i^{th} thermal amplitude variation of the mission profile.
λ_3 : base failure rate of the integrated circuit package. See Table 17a and 17b
π_I : influence factor related to the use of the integrated circuit (interface or not).
λ_{EOS} : failure rate related to the electrical overstress in the considered application..

Technological structure	Temperature factor π_t
MOS BiCMOS (low voltage)	$e^{\left[A\left(\frac{1}{328}-\frac{1}{273+t_j}\right)\right]}$ A=3480 ; (Ea=0.3 eV)
Bipolar BiCMOS (high voltage)	$e^{\left[A\left(\frac{1}{328}-\frac{1}{273+t_j}\right)\right]}$ A=4640 ; (Ea=0.4 eV)
AsGa Numerical	$e^{\left[A\left(\frac{1}{373}-\frac{1}{273+t_j}\right)\right]}$ A=3480 ; (Ea=0.3 eV)
AsGa MMIC	$e^{\left[A\left(\frac{1}{373}-\frac{1}{273+t_j}\right)\right]}$ A=4640 ; (Ea=0.4 eV)
t_j = Junction temperature in °C .	

Mathematical expression of the influence factor Π_α	$\pi_\alpha = 0.06 \times \left\|\alpha_S - \alpha_C\right\|^{0.68}$
Mismatch between substrate and package for the thermal expansion coefficient	$\left\|\alpha_S - \alpha_C\right\|$
α_S	See Table 14
α_C	See Table 14

Interface circuits Typical calculated values			λ_{EOS} FIT	π_I
Function	**Electrical environment**			
Interfaces	Computer		10	1
	Telecoms	switching	15	1
		transmitting, access, subscriber cards	40	1
		subscriber equipment	70	1
	Railways, payphone		100	1
	Civilian avionics (on board calculators)		20	1
	Voltage supply, Converters		40	1
Non Interfaces	All electrical environment		-	0

Mathematical expression of the Influence factor $(\pi_n)_i$	$n_i \le 8760$ Cycles/year	$(\pi_n)_i = n_i^{0.76}$
	$n_i > 8760$ Cycles/year	$(\pi_n)_i = 1.7 \times n_i^{0.60}$
n_i : Annual number of cycles with the amplitude ΔT_i		
For an on/off phase	$\Delta T_i = \left[\frac{\Delta T_i}{3} + (t_{ao})_i\right] - (t_{ao})_i$	
For a permanent working phase, storage or dormant	ΔT_i =average per cycle of the (t_{ac}) variation, during the i^{th} phase of the mission profile.	

「IEC/TR 62380より引用」

JEITA

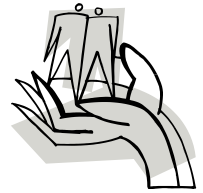
フォールトの分類

デュアル・ポイント・フォールト
(Dual Point Fault)

他の独立したフォールトが重なる（IF+SM)と
安全目標侵害

高リスク

低リスク



SPF
RF

DPF

Latent

Perceived & Detected

Safe
Fault

潜在

知覚できる(Perceived)
検出できる(Detected)

シングル・ポイント・フォールト
(Single Point Fault)

単独のフォールトで安全目標侵害

残存フォールト
(Residual Fault)

SMで処置されないSPFの残り

安全側フォールト

・安全目標を侵害しないフォールト
・N>2となるマルチプルポイントフォールト

ハードウェアメトリクスの評価

SPFM（Single Point Fault Metric）= 1- β/α %

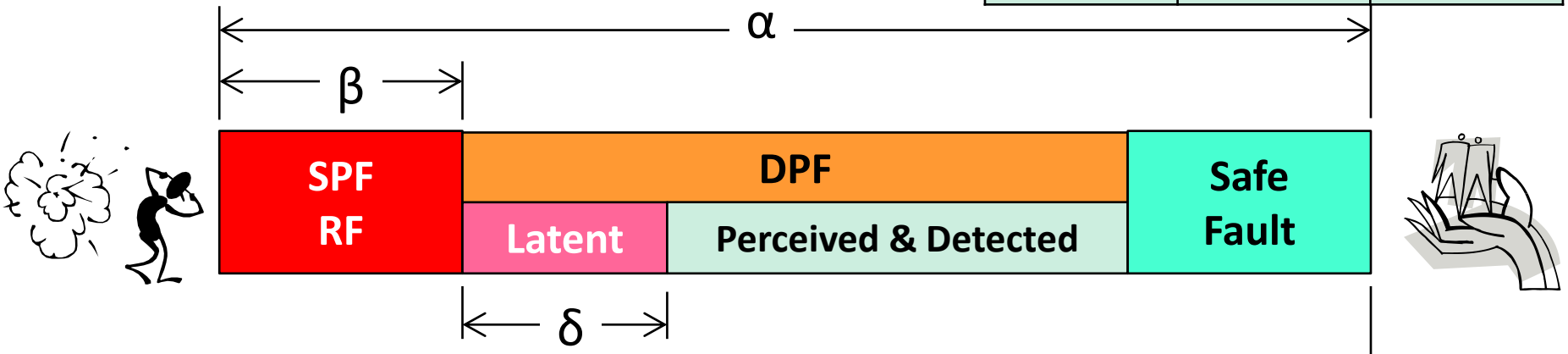
ASIL B	ASIL C	ASIL D
≧90%	≧97%	≧99%

LFM（Latent Fault Metric）= 1- δ/(α-β) %

ASIL B	ASIL C	ASIL D
≧60%	≧80%	≧90%

PMHF（Probabilistic Metric for random Hardware Failures）= β+δ fit

ASIL B	ASIL C	ASIL D
< 100fit	< 100fit	< 10fit



発注元の要求とサプライヤの対応

サプライヤ開発の範囲	発注元 →	サプライヤ
ソフトウェアを含むシステム開発	● 安全目標(ASIL) ● 安全要求 ● DIA(開発インタフェース協定)による責任分担の契約	■ ISO26262に沿った開発 ■ 安全ケースの提出
ASICなどの複雑な構成の素子 複雑さの定義がなく、境界が曖昧	● 安全目標(ASIL) ● 安全要求 ● DIA(開発インタフェース協定)による責任分担の契約	■ ISO26262に沿った開発 ■ 故障モードの分析と情報の提供 ■ 安全マニュアルの提出
受動部品などの単純な素子 ※機能安全要求が無い場合	● 明示的な機能安全要求なし ● 故障モード、按分、故障率の提出要求(場合による)	■ TS16949に沿った開発 ■ 部品仕様の提出 ■ 信頼性評価結果の実施

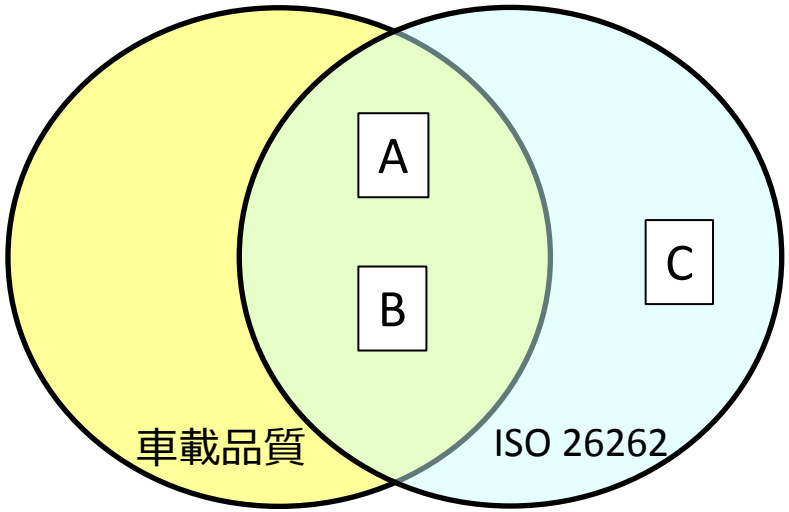
TS16949:自動車製造や関連する交換部品に携わる組織にISO 9001を適用する際の要求事項

まとめ

A:これまでの“車載品質”が基本
- “フェールセーフ”
- “過去トラ”対応
- 高信頼設計の再利用

B:定量的な品質マネジメントシステムが基本
- ASILに基づく品質マネジメントシステム
- 正しい作業の実施による人的ミスの防止
- 客観的な証拠を残す

C:新規に追加される作業
- 安全ケースの作成
- 確証方策の実施
- ハードウェア故障に対する定量的評価とソフトウェアのテスト網羅の評価



Q&A