1．サプライヤ視点からの機能安全対応

本日の内容

1．サプライヤ視点からの機能安全対応

- 要旨
  - ・ 先ずは、最新の動向も踏まえた機能安全の概要を紹介します
  - ・ 併せて、機能安全対応のポイントや課題をいくつか解説します
  - ・ 今後の御社の機能安全対応へご参考いただければ幸いです
- 内容
  - (1) 自動車版の機能安全(ISO 26262)の概要
  - (2) 自動車業界の機能安全対応の現状
  - (3) サプライヤ領域の機能安全対応のポイント
  - (4) 機能安全対応の今後の課題

サプライヤ視点からの機能安全対応

(1) 自動車版の機能安全(ISO 26262)の概要

(2) 自動車業界の機能安全対応の現状

(3) サプライヤ領域の機能安全対応のポイント

(4) 機能安全対応の今後の課題

(1) 自動車版の機能安全(ISO 26262)の概要

・ 導入の背景(モビリティ社会のニーズ)

地球環境

■地球にやさしい環境作りへの貢献

■温暖化防止に向けたCO2排出量低減、燃費改善、エネルギー多様化

■電動化(ハイブリッド、PHV、EV)

交通安全

■交通事故ゼロ社会の実現

■衝突安全～予防安全～運転支援

■普及のための既存製品の低コスト化と更なる先進安全装備の開発

将来社会

■家や地域とエネルギー連携スマートグリッド、マイクログリッド

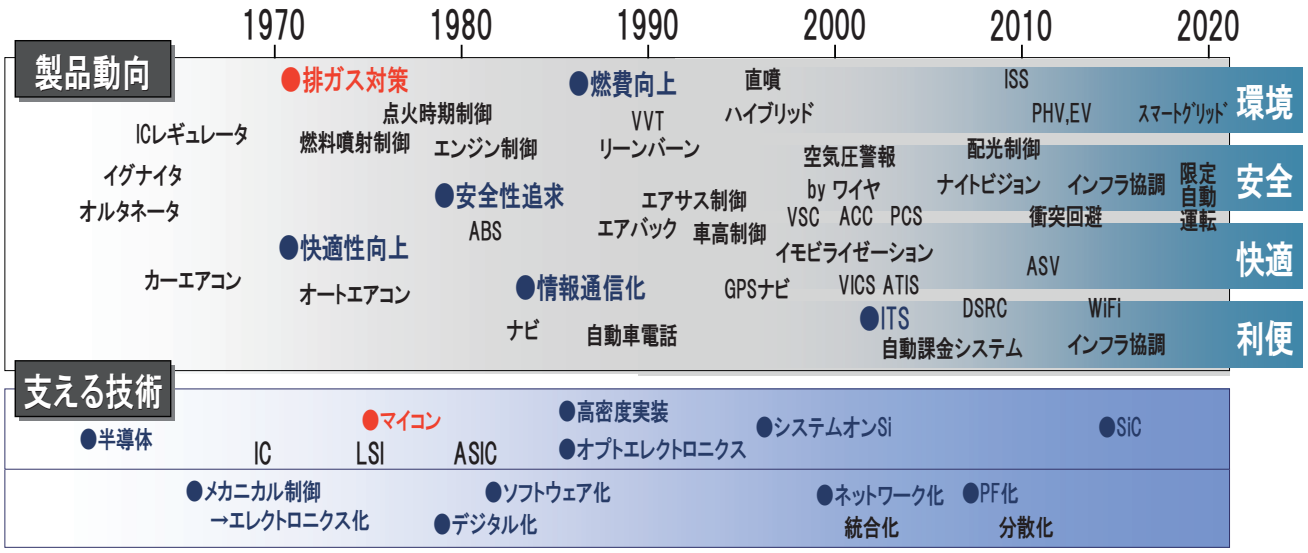
■インフラ協調(車車、路車)による半自動運転

■利用スタイルの変化(カーシェアリング、マルチモーダル)

同様に制御連携、電動化、インフラ協調に伴う機能進化

(1) 自動車版の機能安全(ISO 26262)の概要

・ 導入の背景(カーエレクトロニクスの発展)



制御／電子システムの高度化、大規模化が進展

(1) 自動車版の機能安全(ISO 26262)の概要

・ 導入の背景(制御/電子システムの課題)

－ 複雑化への対応

システムの複雑化

- ■機能、使い方の複雑化
- ■制御構造の複雑化
- ■システム構成の複雑化
- ■ソフトウェアの複雑化
- ■マイコン、ASIC実装の複雑化
- ・・・

プロセスの複雑化

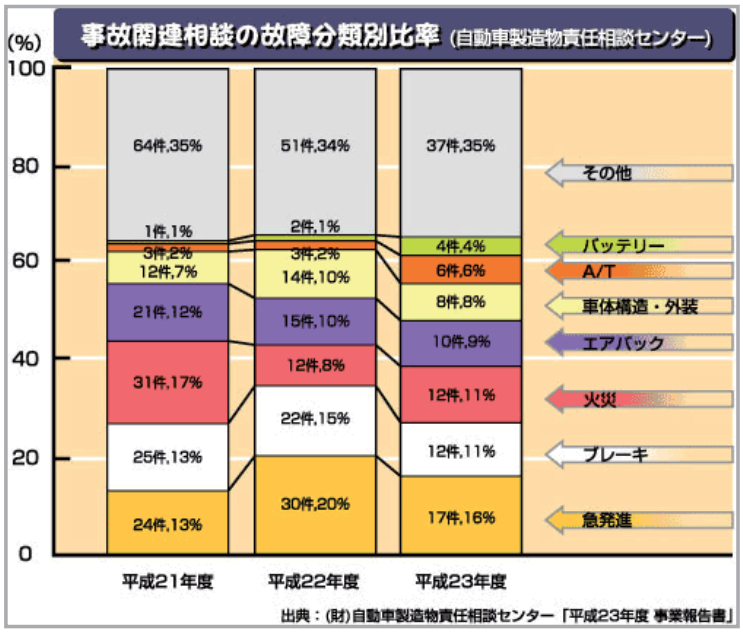
- ■工程数、関連工程の複雑化
- ■設計者関係の複雑化
- ■マネジメント体系の複雑化
- ■責任、役割分担の複雑化
- ・・・

複雑化(大規模化かつ容易性の低下)への対応

(1) 自動車版の機能安全(ISO 26262)の概要

・ 導入の背景(市場・ユーザの声)

出典:JAF http://www.jaf.or.jp/qa/others/recall/02.htm



JAFコメント:

自動車事故はスピードの出し過ぎ、
不注意などのユーザー起因がほとんど

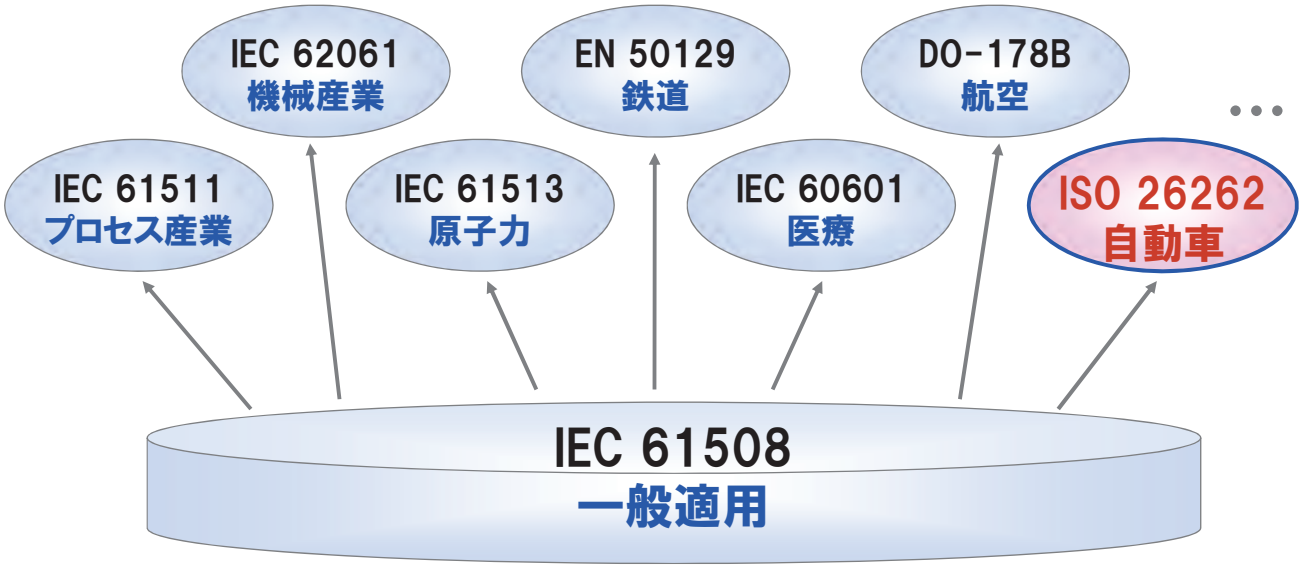
一方でクルマ自体の不具合によって
発生したケースも皆無ではない

現に、ブレーキやアクセルの不具合
によって他車にぶつかってしまった
ケースの事故も起きている

業界対応を望む声

(1) 自動車版の機能安全(ISO 26262)の概要

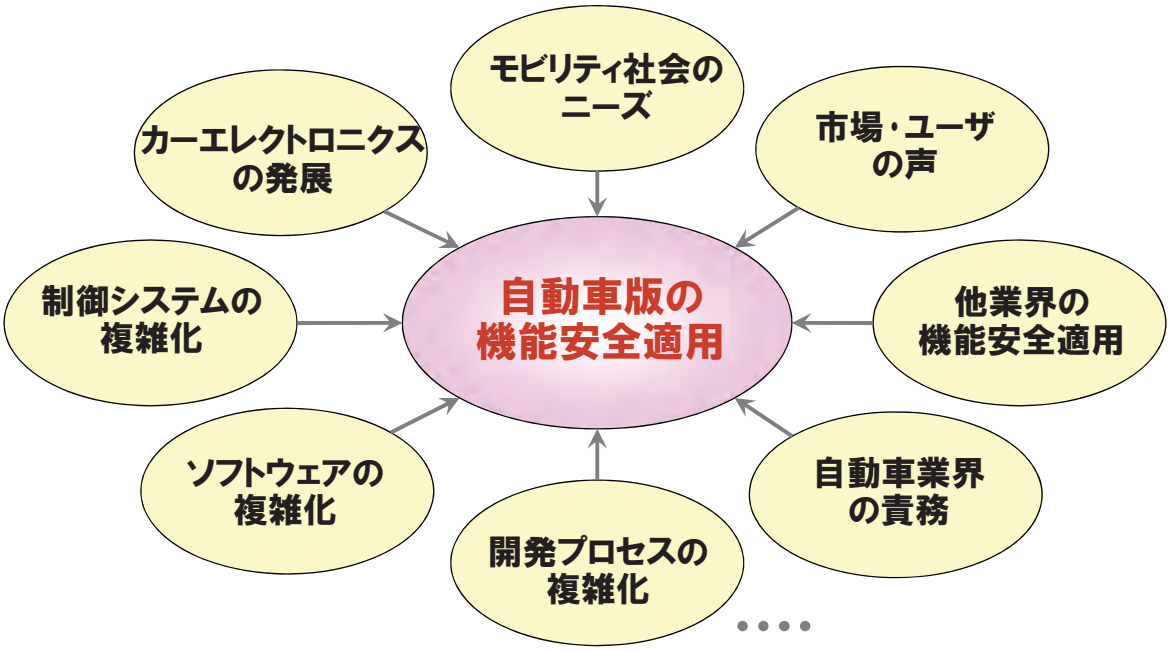
・ 導入の背景(他業界の対応)



自動車業界への安全に対する取組み要請

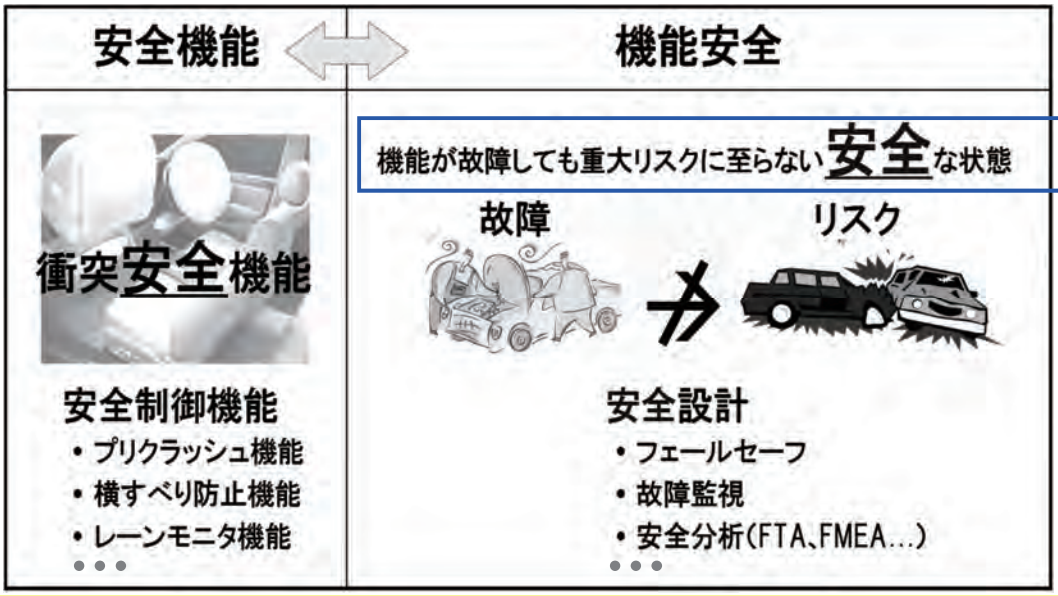
(1) 自動車版の機能安全(ISO 26262)の概要

- 導入の背景(まとめ)



(1) 自動車版の機能安全(ISO 26262)の概要

- 機能安全の意味

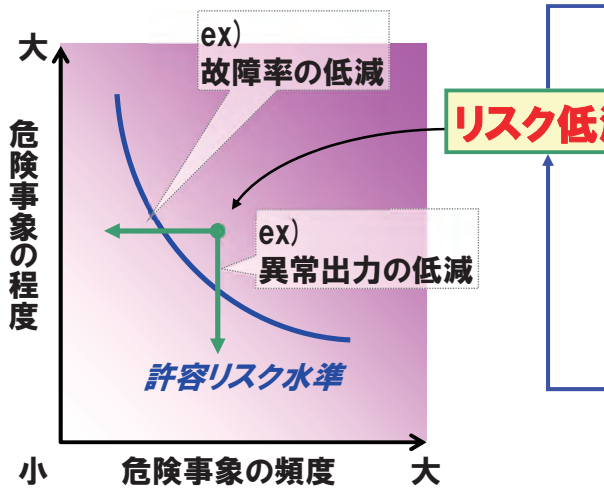


故障や異常によるシステムの機能不全を防ぐ/低減する

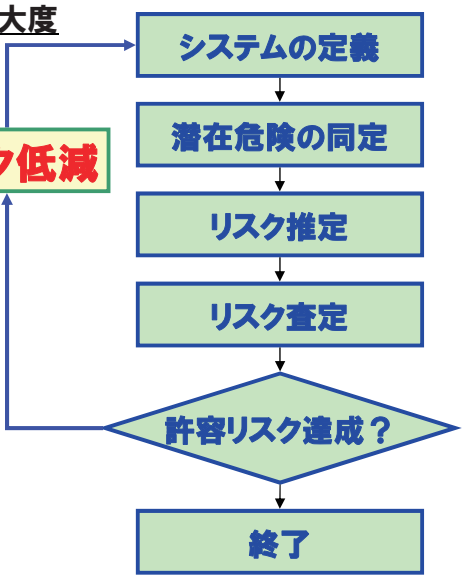
(1) 自動車版の機能安全(ISO 26262)の概要

・ 機能安全の考え方

リスク ＝ 危険事象の頻度 × 危険事象の重大度



リスク低減のフロー



「リスクベースのアプローチ」が基本の考え方

(1) 自動車版の機能安全(ISO 26262)の概要

・ ISO 26262(規格概要)

- 名称
  - Road vehicles — Functional safety —
- 制定
  - 2011年 11月15日
- 適用
  - 制定日以降の新規開発車両～

自動車業界特有の難しさ
■多様性の考慮が必要(場所・人)
■制約が少ない(一般向け・非管理下)
他…

一般消費者向けの量産製品として初めての適用

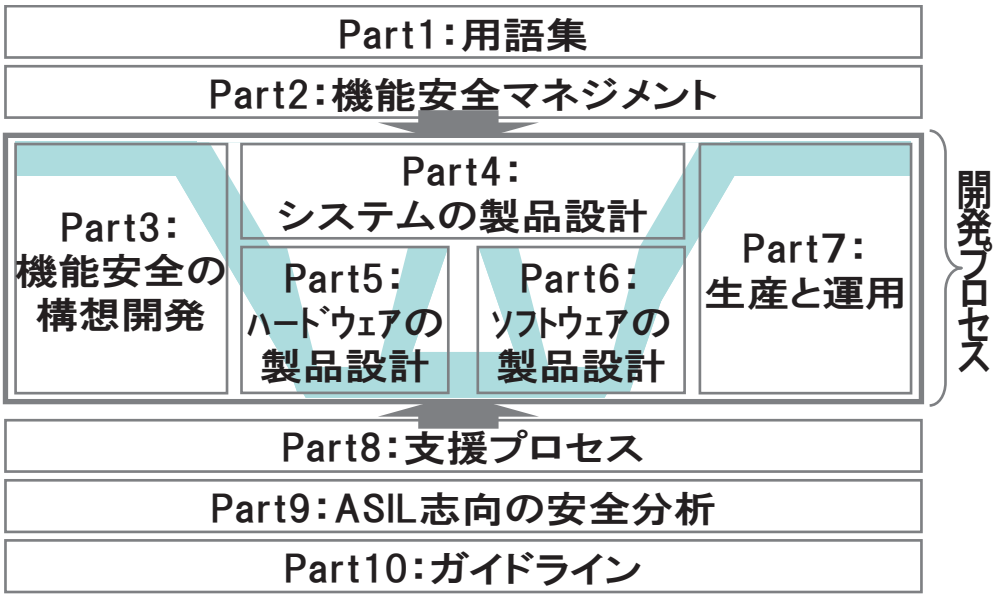
(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262(規格主旨)
  - 自動車分野の**安全ライフサイクルの定義**と、各フェーズのテーラリングを許容
  - 自動車固有の**リスク等級(ASIL)の設定**と、リスクベースの手法を提供
  - **残存リスクの許容水準への抑制**と、ASILに沿った安全要求の導出
  - 許容水準の抑制の達成を図るための、**確認レベルと確認者の独立性**に対する規格要件を提供
  - **OEMとサプライヤとの関係**に対する規格要件を提供

考え方～詳細技法の細部までの幅広い観点から規格要件を提供

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262(Part構成)



V字プロセスモデルと関連するマネジメント・プロセス・技法で構成

(1) 自動車版の機能安全(ISO 26262)の概要

・ ISO 26262(適用範囲)

・対象車両

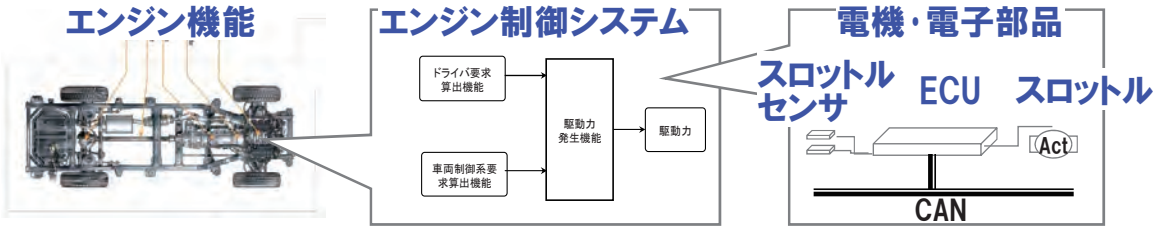
最大総重量 3.5t 以下の乗用車 （通常は、二輪車、大型車、特殊車両は含まない）

・対象システム

「システムの機能失陥 ⇒ 危険な状態」 の可能性がある機能、システム

・対象部品

電機・電子系部品 （通常は、センサやモータのメカ構造部は含まない）



機能失陥が「危険な状態」へ至る可能性があるシステム

(1) 自動車版の機能安全(ISO 26262)の概要

・ ISO 26262の特徴

- ASIL：Automotive Safety Integrity Level(安全性指標)
  - ASIL A～Dの4段階
  - ハザードがASIL Aに満たない機能：
    QM(Quality Management)
  - 機能不全状態に対し、3つのパラメータを設定する
    - E：Exposure　　運転状況
    - C：Controllability　　回避操作性
    - S：Severity　　人体に及ぶ危害度

ハザードは、ASILによって4つのレベルに層別されている

(1) 自動車版の機能安全(ISO 26262)の概要

・ ISO 26262の特徴

－ ASIL:パラメータの設定基準

E1	E2	E3	E4
極めて低い確率(年1回)	低い確率(1%未満)	中程度の確率(1～10%)	高い確率(10%)

C1	C2	C3
簡単に制御可能(99%以上の人が回避できる)	普通に制御可能(90%以上の人が回避できる)	制御が難しい，制御不能(回避できるのは90%未満)

S1	S2	S3
軽傷～中程度の障害	生存の見込みはあるが重い障害(90%以上は生存見込みあり)	生命を脅かす障害，致命傷(生存見込みなしが10%を超える)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

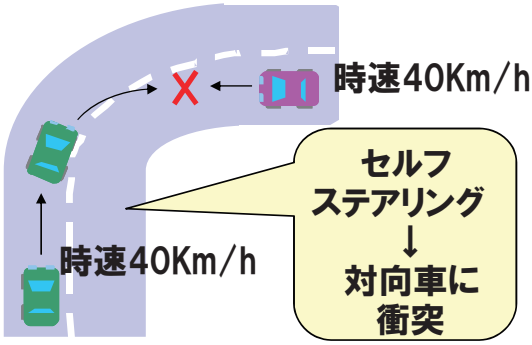
(1) 自動車版の機能安全(ISO 26262)の概要

・ ISO 26262の特徴

－ ASIL:設定事例

電動パワーステアリング

・機能故障 ： モーター制御異常
・ハザード ： セルフステアリング
（意図しないアシストトルクの発生）



パラメータ	分析結果		判定
運転状況	中央分離帯なしのカーブ	10%以上の遭遇頻度	E4
操作回避性	ステアリング操作困難	10%以上が回避不能	C3
人体へ及ぶ危害度	相対速度80km/h	90%以上の致命傷	S3

⇒ ASIL-D

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - ASIL：主なハザードのASIL事例

同じハザードでも、車両機構や装備等により、ASILが異なる場合がある

機能分類	ハザード事象	ASIL
走る	急発進	B～D
	急加速	B～D
	駆動機能の喪失	QM～C
止る	急制動	C～D
	1輪制動	D
	制動機能の喪失	C～D
曲る	セルフステア	D
	ステアリングロック	C～D
	アシストの喪失	A～C
見る	視界不良	QM～B
	視界の喪失	A～B

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Safety requirement(安全要求)

下記設計階層を更に分割する場合がある
ex) システム設計 > サブシステム設計

設計階層	安全要求	内容
車両設計	安全目標	車両、ドライバーに対する安全な状態
機能設計	機能安全要求	上記を実現するための、機能/制御の振舞い
システム設計	技術安全要求	上記を実現するための、車両部品/電子システムの動作
製品設計	ハードウェア安全要求 ソフトウェア安全要求	上記を実現するための、ハード/ソフトウェアの処理

設計階層に沿って上位から下位へ安全要求を具体化する

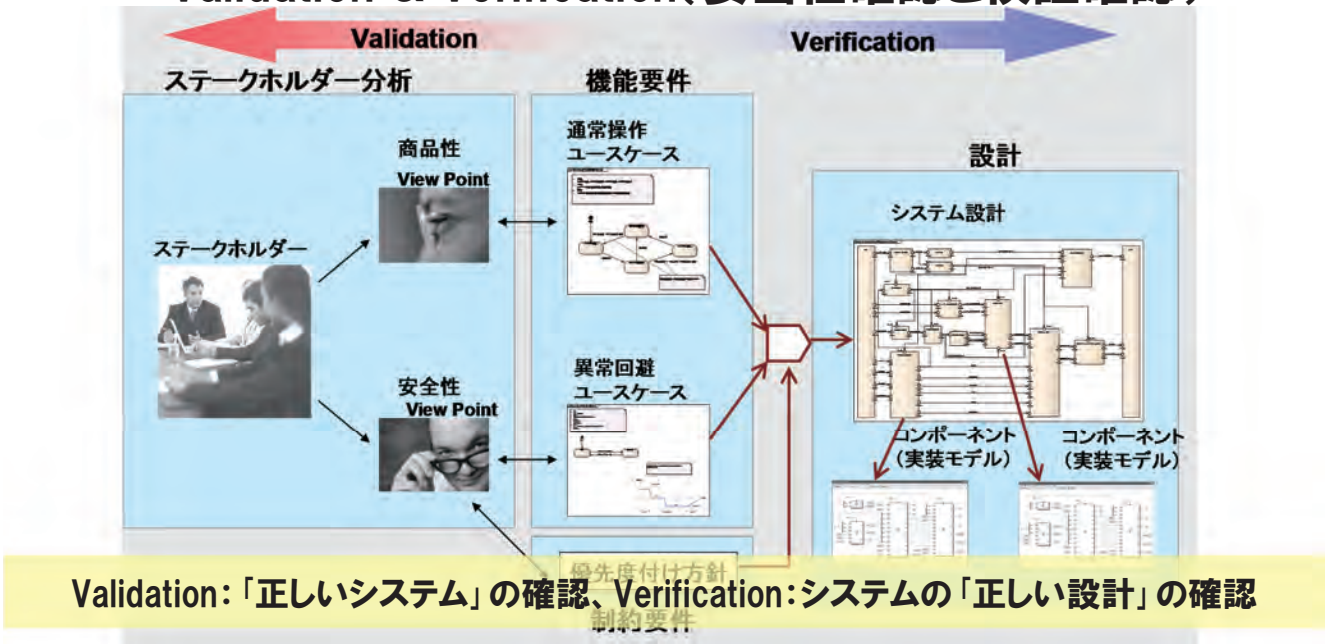
(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Safety analysis(安全分析)
    - 安全分析の目的
      - 対象機能のハザードを抽出する
        - 主な手法:HAZOP、システムFMEA…
      - 安全要求として対処すべき異常や故障を網羅的に抽出する
        - 主な手法:FMEA、FMEDA…
      - 設計階層間の異常や故障の因果関係を明確にする
        - 主な手法:FTA、ETA…

ハザード対処の妥当性・網羅性および論証の裏づけ

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Validation & Verification(妥当性確認と検証確認)



Validation:「正しいシステム」の確認、Verification:システムの「正しい設計」の確認

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Documentation(文書化)

対象文書の一例

	計画	安全分析	安全要件	設計	テスト設計	各種報告
1) 対象機能の安全構想	安全計画書 V&V計画書	ハザード解析 リスク評価(ASIL設定)	機能安全構想書		機能テスト設計書	車両機能テスト報告書
2) システムの開発＆設計	システム開発計画書 システムV&V計画書	システムFT システムFMEA	システム安全要件書	システム安全設計書	システムテスト設計書	システムテスト報告書
2) ECUの開発＆設計	ECU開発計画書 ECU V&V計画書	ECU FT ECUの故障・診断率	ECU安全要件書	ECU安全設計書	ECUテスト設計書	ECUテスト報告書
3) ハードウェア開発＆設計	ハード開発計画書 ハードV&V計画書	素子FME 素子故障・診断率	ハード安全要件書	ハード安全設計書	ハードテスト設計書	ハードテスト報告書
4) ソフトウェア開発＆設計	ソフト開発計画書 ソフトV&V計画書	ソフトFME 各種カバレッジ	ソフト安全要件書	ソフト安全設計書	ソフトテスト設計書	ソフトテスト報告書
5) 生産＆市場	生産準備計画書		生産準備安全要件書		生産	テスト報告書

設計階層毎の文書化(設計の適確性/網羅性を示すエビデンス)

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - DIA:Development Interface Agreement(開発分担)
    - DIAとは？
      - 顧客とサプライヤ間の開発単位毎に取交される、活動/証拠/成果物に対する役割・責任の合意事項
    - DIAの目的
      - 対象機能の開発において、カーメーカ⇔サプライヤ間の分散開発のマネジメントが適確にできていることを示す
      - 分散開発における各種取決め(特に役割と責任の分担)を明示して開発管理を進める

プロジェクト毎に両者で合意し取交しをする合意書

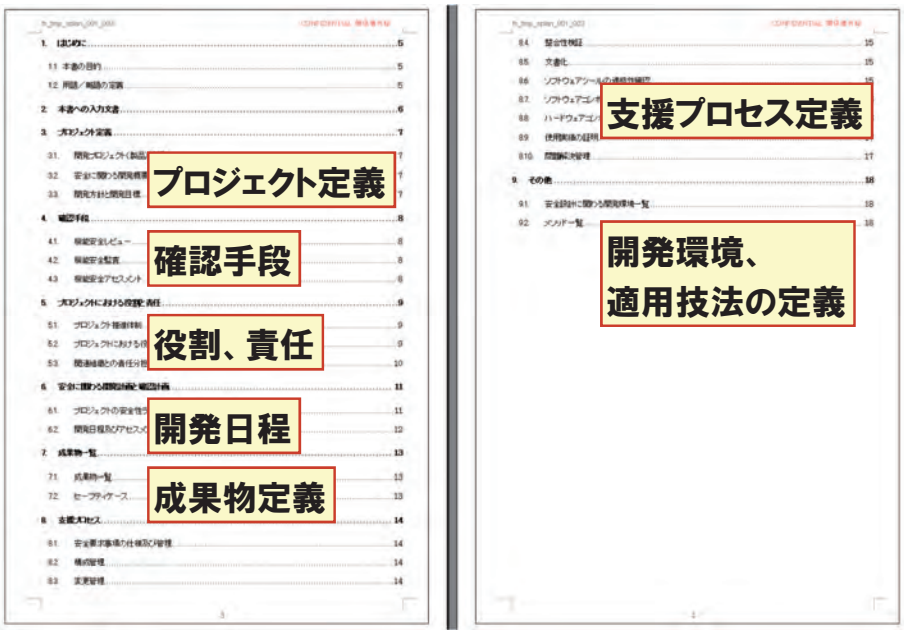
(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Safety plan(安全計画)
    - 安全計画書とは？
      - 安全ライフサイクルに沿った**プロジェクト活動の全体像と成果物の作成計画**を示す文書
        - » 開発方針、プロジェクト組織＆メンバ、日程計画、開発環境(ツール等)…
    - 安全計画書の目的
      - **プロジェクト活動の明示**とメンバ間の共有
      - **分散開発者との整合確保**

「ISO 26262へ準拠したプロジェクト活動」を示す文書

(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Safety planの事例



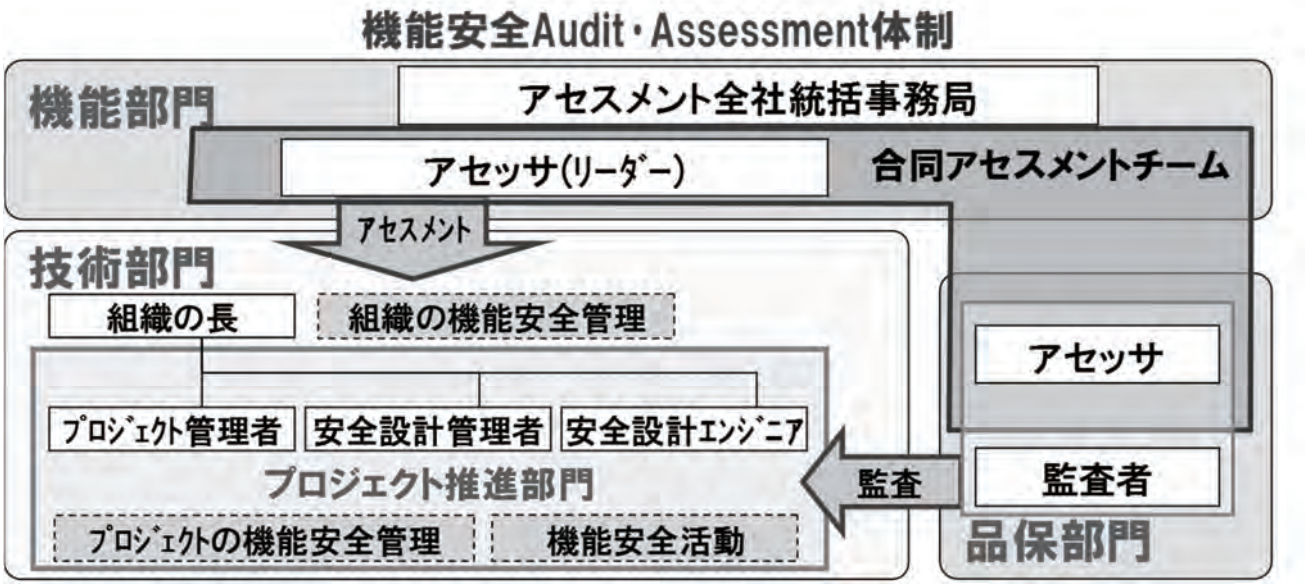
(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Functional Safety Audit & Assessment
    - Functional Safety Auditとは？
      - 対象のプロジェクトが、**組織が定めた規程、開発プロセスを満たして活動**していることを確認
    - Functional Safety Assessmentとは？
      - ①組織の規程、開発プロセスが機能安全規格に準拠していること
      - ②プロジェクトの活動とその成果物が機能安全規格に準拠していること
      - 上記の確認結果とレビュー、監査の結果も考慮し**機能安全活動の総合的な評価**を行う

製品／プロセス両面で独立性のある部門が実施

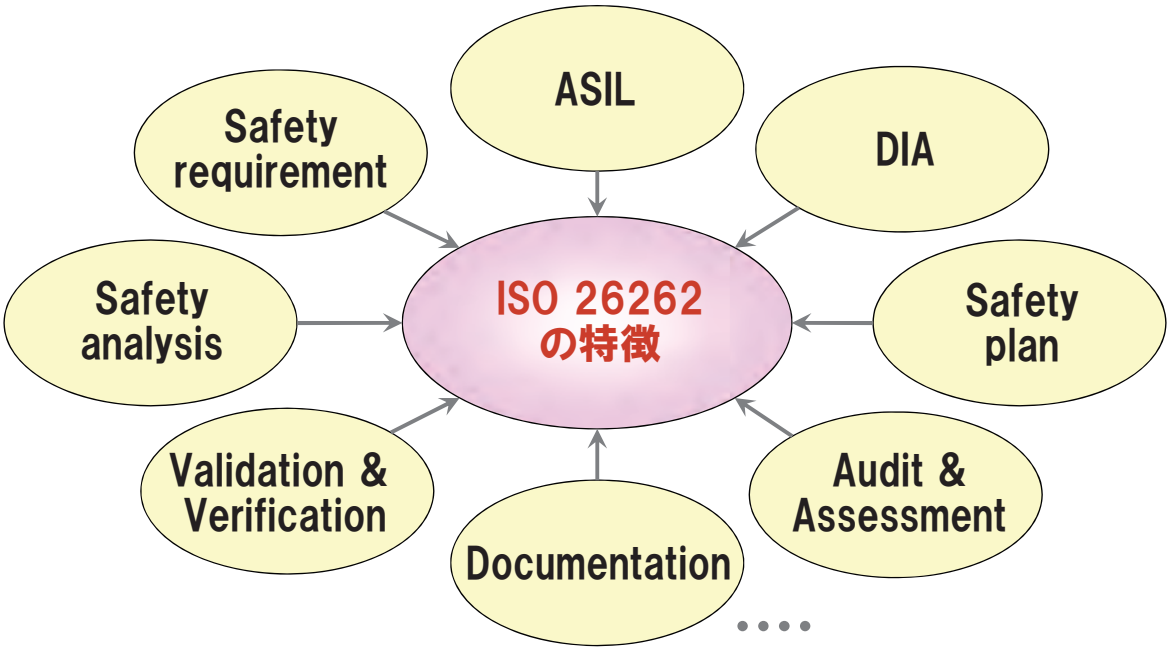
(1) 自動車版の機能安全(ISO 26262)の概要

- ISO 26262の特徴
  - Functional safety Audit & Assessmentの体制事例



(1) 自動車版の機能安全(ISO 26262)の概要

・ ISO 26262の特徴(まとめ)



サプライヤ視点からの機能安全対応

(1) 自動車版の機能安全(ISO 26262)の概要

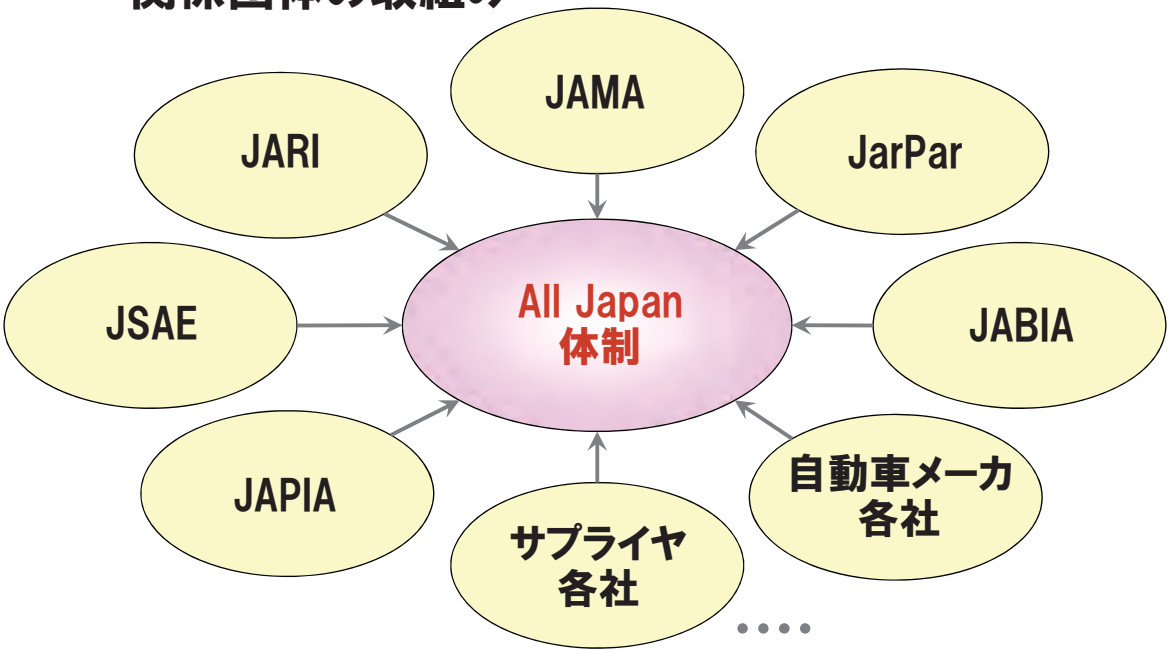
(2) 自動車業界の機能安全対応の現状

(3) サプライヤ領域の機能安全対応のポイント

(4) 機能安全対応の今後の課題

(2) 自動車業界の機能安全対応の現状

- 国内動向
  - 関係団体の取組み



(2) 自動車業界の機能安全対応の現状

- 国内動向
  - OEMの取組み
    - 乗用車メーカ
    - トラックメーカ、二輪メーカ
  - サプライヤの取組み
    - Tier1/Tier2サプライヤ
    - 電子系部品関連サプライヤ
  - 関連ベンダの取組み
    - 部品/ソフト ベンダ
    - ツールベンダ

(2) 自動車業界の機能安全対応の現状

- 欧州動向
  - 関係団体の取組み
    - VDA、BNA…
  - OEMの取組み
    - ドイツOEM、フランスOEM、その他OEM…
  - サプライヤの取組み
    - メガサプライヤ、Tier1/2サプライヤ…
  - 関連ベンダの取組み
    - 大手半導体ベンダ、大手ツールベンダ…

(2) 自動車業界の機能安全対応の現状

- 北米動向
  - 関係団体の組み
    - SAE
  - OEMの取組み
    - Big3
  - サプライヤの取組み
    - メガサプライヤ、Tier1/2サプライヤ
  - 関連ベンダの取組み
    - 大手半導体ベンダ、大手ツールベンダ…

サプライヤ視点からの機能安全対応

(1) 自動車版の機能安全(ISO 26262)の概要

(2) 自動車業界の機能安全対応の現状

(3) サプライヤ領域の機能安全対応のポイント

(4) 機能安全対応の今後の課題

(3) サプライヤ領域の機能安全対応のポイント

・ 対応方針の明確化

よくある機能安全導入時の困り事

■何から手をつけてよいのか見えてこない

■どこまでやり切ればよいのか分からない

■掛け声だけで、具体的な進展が少ない

■多くの労力が掛かる割りに、メリットが探せない

■…

→ 対応方針の明確化が必要

広範囲に及ぶ機能安全は、対応方針の明確化が必要

(3) サプライヤ領域の機能安全対応のポイント

- 対応方針の分類
  - プロセス、マネジメントのポイント
    - トップマネジメントとしての　A) 会社方針
    - 組織/プロジェクトとしての　B) 実用方針
  - 製品技術・技法のポイント
    - 対象アイテムに適した　C) 安全構想
    - 考え方や背景を反映した　D) 安全要求

会社／プロジェクトそれぞれの対応レベルを定める

(3) サプライヤ領域の機能安全対応のポイント

- 対応方針の分類
  - プロセス、マネジメントのポイント
    - トップマネジメントとしての　A) 会社方針
    - 組織/プロジェクトとしての　B) 実用方針
  - 製品技術・技法のポイント
    - 対象アイテムに適した　C) 安全構想
    - 考え方や背景を反映した　D) 安全要求

(3) サプライヤ領域の機能安全対応のポイント

A) 会社方針の事例

① 適用方針

i. 適用目的 ☞事例
ii. 適用効果 ☞事例
iii. 適用目標
iv. 適用時期 ☞事例
v. 適用範囲
vi. 適用レベル
…

② 展開方針

i. 展開指示 ☞事例
ii. 展開方法
iii. 展開部隊
iv. 展開手段
v. 展開支援
…

機能安全対応の取組みに対する方針明確化

(3) サプライヤ領域の機能安全対応のポイント

① 機能安全対応の適用方針

事例☞ i. 適用目的

・ 機能安全を適用することの会社レベルの目的を設定する

積極的な目的
■安全性確保の一手段
■安全設計の改善へ活用
■…

…

中間レベル
■CSR
■…

…

通常目的
■規格準拠を示す
■調達要件の達成
■…

ポイント：会社レベルの適用目的の設定

(3) サプライヤ領域の機能安全対応のポイント

① 機能安全対応の適用方針

事例☞ ii. 適用効果

・ 機能安全を適用する効果や狙いを設定する

明示的な効果	中間レベル	特になし
■新規ビジネス ■売り込み材料 ■…	■プロセス改善 ■…	■対応に伴う労力のみ ■…

ポイント：機能安全対応で得られる効果の明示化

(3) サプライヤ領域の機能安全対応のポイント

① 機能安全対応の適用方針

事例☞ iv. 適用時期

・ 機能安全を適用する時期を設定する

早い時期	中間レベル	遅い時期
■直ちに適用 ■立ち上がり機種の多い〇〇年△△月～ ■…	■顧客から明確な適用要請があった時点～	■##年以降に開発する□□製品～ ■当面予定なし ■…

ポイント：会社としての適用時期のガイドライン化

(3) サプライヤ領域の機能安全対応のポイント

② 機能安全対応の展開方針

事例☞ i. 展開指示

・ 展開活動を進めるための後ろ盾を明確にする

トップ層	…	中間レベル	…	明示なし
■社長指示 ■担当役員指示 ■…		■部門長指示 ■…		■自主活動 ■…

ポイント：展開活動のスポンサー、支援者、後ろ盾

(3) サプライヤ領域の機能安全対応のポイント

B) 実用方針の事例

③ 組織レベル

i. プロセス整備 ☞事例
ii. 体制構築
iii. 教育体系 ☞事例
iv. ツール活用
…

④ プロジェクトレベル

i. OEM/サプライヤの分担
ii. 各種計画書
iii. 確証方策
…

機能安全対応の取組みに対する方針明確化が重要

(3) サプライヤ領域の機能安全対応のポイント

③ 組織レベルの実用方針

事例☞ i. プロセス整備

・ ギャップ分析の結果を反映し、整備範囲やレベルを定める

ゼロベース
- ■新規プロセスの導入
- ■A-SPICEへの置換え
- ■…

…

部分改善
- ■既存プロセスへ必要分を追加
- ■…

…

一部修正
- ■ギャップが大きい工程のみ修正
- ■…

ポイント：ギャップ分析結果から整備方針を定める

(3) サプライヤ領域の機能安全対応のポイント

③ 組織レベルの実用方針

事例☞ iii. 教育体系

・ 必要な知識や情報を補う為の教育体系を整備する

再構築
- ■機能安全用の教育体系を再構築
- ■…

…

現状への組込み
- ■必要な教育を補填する
- ■…

…

特になし
- ■組織レベルの教育は未実施
- ■外部教育活用
- ■…

ポイント：新規/既存、内部/外部を考慮した整備方針を定める

(3) サプライヤ領域の機能安全対応のポイント

- プロセス・マネジメントのポイント(まとめ)
  - トップマネジメントとしての　A) 会社方針
    - 会社レベルの適用目的の設定
    - 機能安全対応で得られる効果の明示化
    - 会社としての適用時期のガイドライン化
    - 展開活動のスポンサー、支援者、後ろ盾

      …
  - 組織/プロジェクトとしての　B) 実用方針
    - ギャップ分析結果から整備方針を定める
    - 新規/既存、内部/外部を考慮した整備方針を定める

      …

(3) サプライヤ領域の機能安全対応のポイント

- 対応方針の分類
  - プロセス、マネジメントのポイント
    - トップマネジメントとしての　A) 会社方針
    - 組織/プロジェクトとしての　B) 実用方針
  - 製品技術・技法のポイント
    - 対象アイテムに適した　C) 安全構想
    - 考え方や背景を反映した　D) 安全要求

(3) サプライヤ領域の機能安全対応のポイント

C) 安全構想設定時のポイント

⑤ 対象アイテムに適した安全構想

- 制御タイプ
  - 連続系システム or 離散系システム
  - 常時稼動 or イベント稼動
- 制御継続性
  - 制御継続 or 縮退制御 or 条件付制御停止 or 制御停止
- 対処のタイミング
  - 異常発生後の対処 or 異常発生前の対処
- デコンポジションの適用可否
  - 複数手段の安全要求(⇒可) or 単一手段の安全要求(⇒否)

対象アイテムに適した安全構想の設定が重要

(3) サプライヤ領域の機能安全対応のポイント

D) 安全要件導出時のポイント

⑤ 安全要求の導出背景の明確化

- OEM要求の反映
  - 疑わしきは止める or 極力動かす
  - 現行の安全構想をキープする／しない
- 対応方針の反映
  - 次世代型まで継続 or 現行のみ、次期型から新規対応
  - 全グレード統一をする／しない
- 設計方針の反映
  - ハードウェアによる監視を充実 or 制御/ソフトによる監視を充実
  - 特定ECUへ安全機構を集約する/分散させる

設計者の意図を反映した安全要求の導出が重要

(3) サプライヤ領域の機能安全対応のポイント

- 製品技術・技法のポイント(まとめ)
  - 対象アイテムに適した　C) 安全構想
    - 制御タイプ
    - 制御継続性
    - 対処のタイミング
    - デコンポジションの適用可否

      …
  - 考え方や背景を反映した　D) 安全要求
    - OEM要求の反映
    - 対応方針の反映
    - 設計方針の反映

      …

サプライヤ視点からの機能安全対応

(1) 自動車版の機能安全(ISO 26262)の概要

(2) 自動車業界の機能安全対応の現状

(3) サプライヤ領域の機能安全対応のポイント

(4) 機能安全対応の今後の課題

(4) 機能安全対応の今後の課題

- 課題観点
  - どこまでやり切ればよいのか？
    - 到達レベル
      - 技術面
      - マネジメント、プロセス面
    - 定着レベル
      - 技術面
      - マネジメント、プロセス面

(4) 機能安全対応の今後の課題

- 課題観点
  - 新しい機能への対応は？
    - 統合制御システム
    - インフラ協調システム
    - 高度運転支援システム

(4) 機能安全対応の今後の課題

- **課題観点**
  - **改訂版(ISO 26262 Edt.2)への備えは？**
    - **二輪車への拡大**
    - **大型(バス･トラック)への拡大**