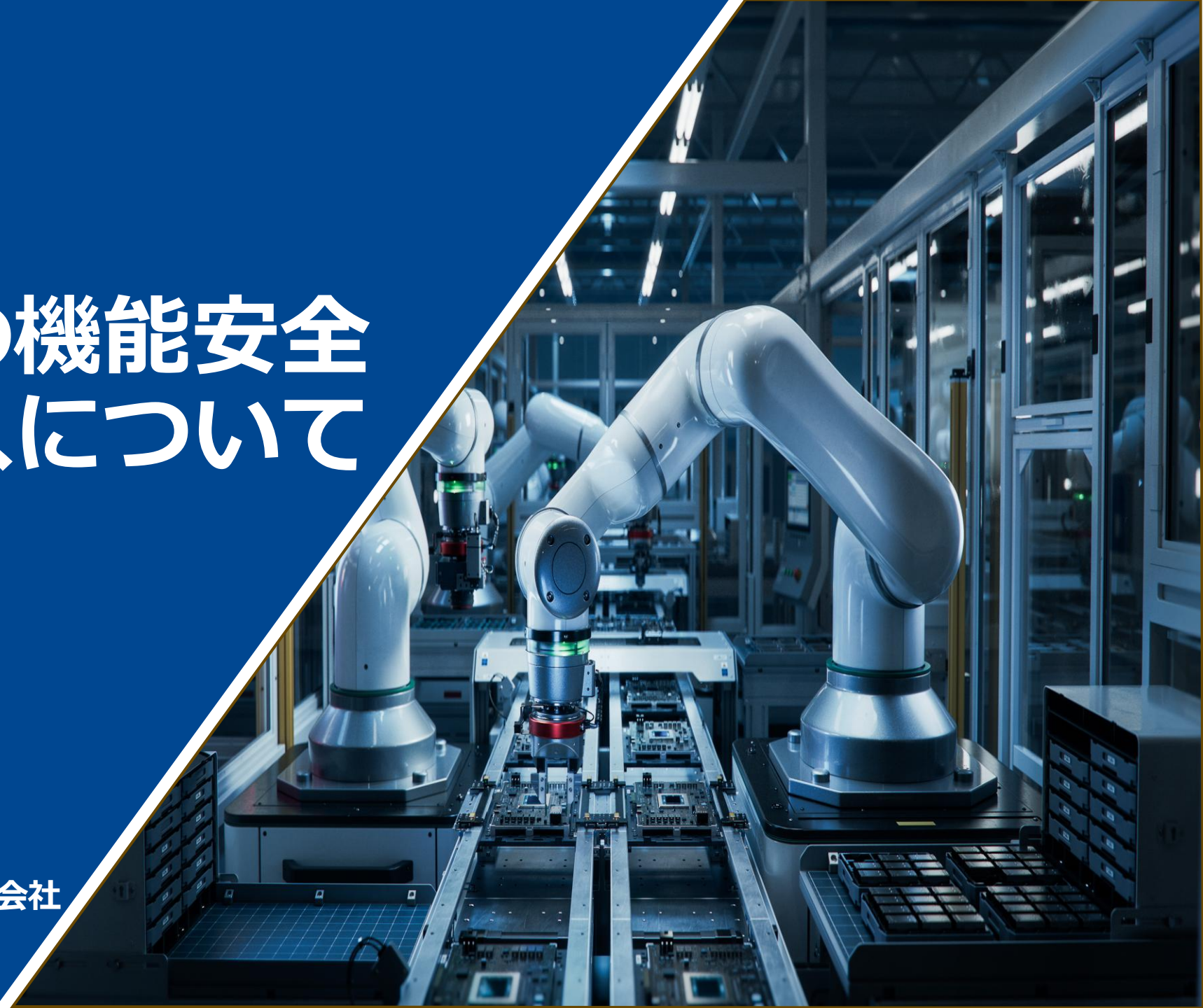
Vtechの機能安全サービスについて



ベリフィケーションテクノロジー株式会社

初めに

機能安全について

機能安全とは、「絶対に壊れない（安全）」ではなく「壊れても事故を起こさない」という考えです。

- 危険要因（不具合）を低減あるいは削除するとの考え方ではなく、“ものは壊れる”との観点に基づき、機能的な工夫（安全を確保する機能）を導入し、許容できるレベルの安全を確保することです。
- 受け入れ可能なリスクに対して、被害の度合いと発生率から計算した定量的な安全度を指標とした製品の安全性を規定します。
- 特に「ISO26262」は、以下も考慮しています。
  - 訴訟リスクの回避
  - 市場ニーズへの対応
  - 法規化の可能性(車載では、既に法規化されている)

- 機能安全とは
- 全体的な安全管理への対応
- 開発プロジェクトへの対応
- LSI開発における 機能安全実績

機能安全とは

安全には２種類ある

■機能安全：冗長性(同質性と異質性)

安全　＝　許安ができないリスクがない事

◆本質安全

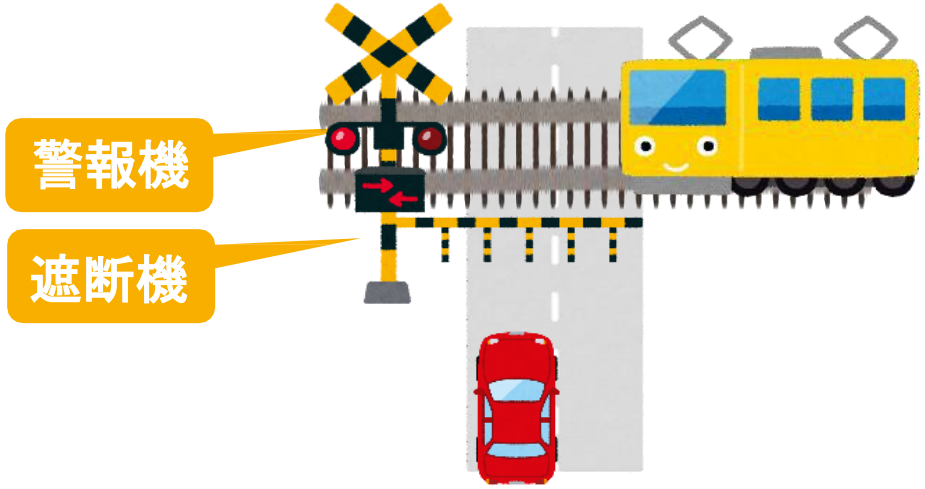
- 人間や環境に危害を及ぼす原因そのものを低減、あるいは除去する事

線路と道路を立体交差にすれば、
事故に遭遇する可能性はない

完全に原因を取り除くことは非現実的

◆機能安全

- 機能的な工夫を導入して、許容できるレベルの安全を確保する事

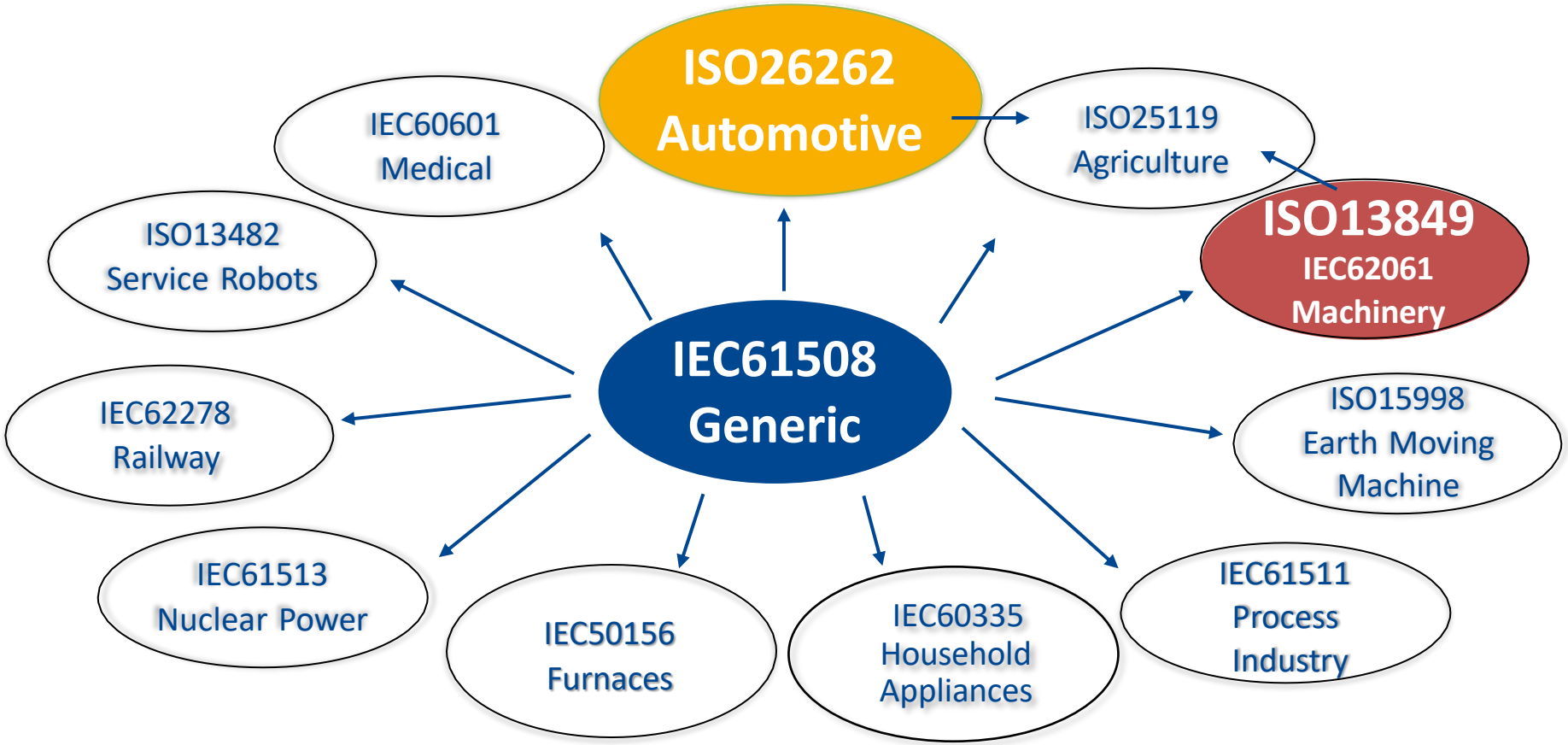


踏切の警報機や遮断機設置により、
許容できるレベルまでリスクを下げる

© 2024 Verification Technology Inc.

機能安全規格の関係

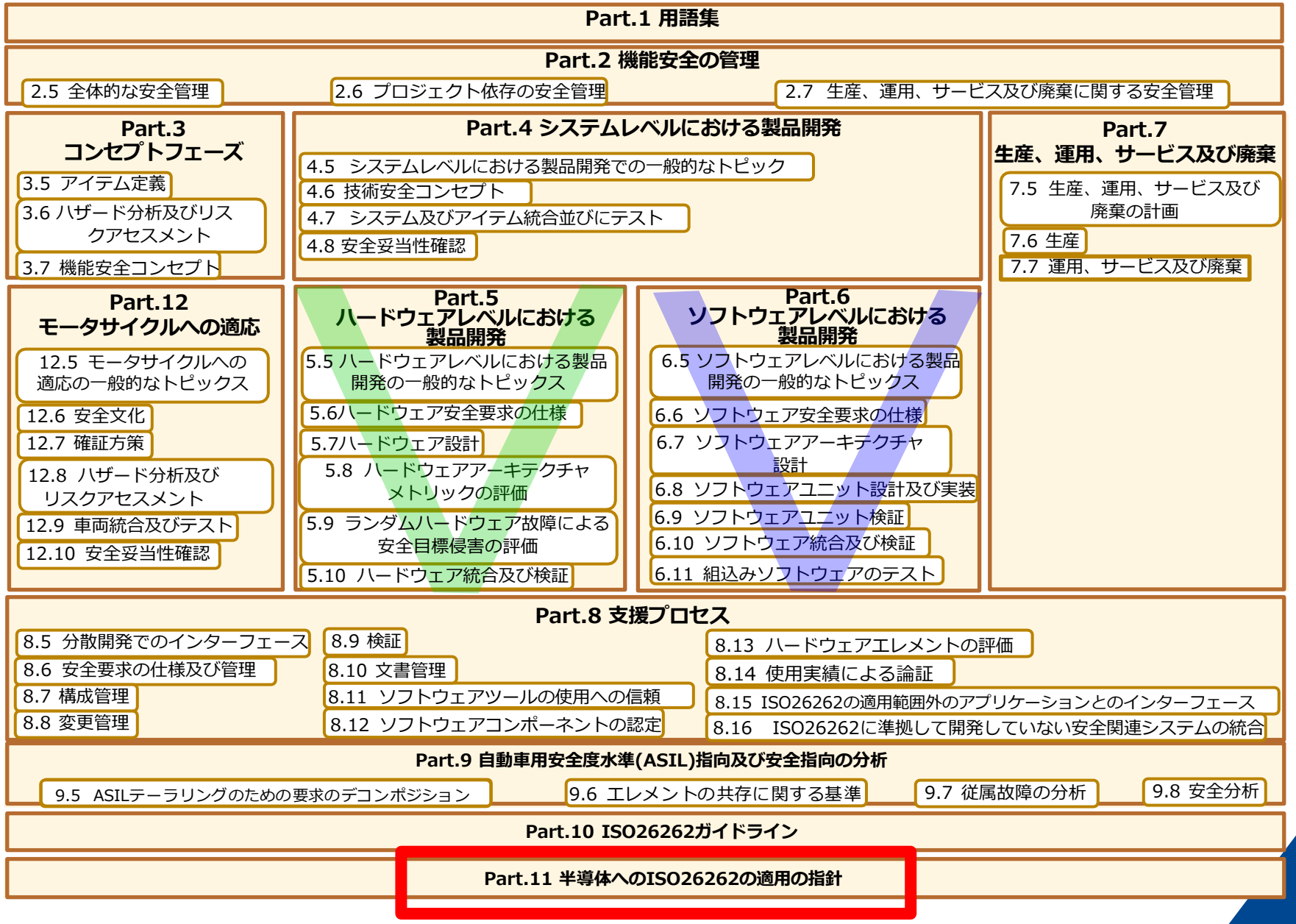
■機能安全の対応分野



◆産業別規格は、ベース規格：IEC61508を参照可能
開発時に求められる要求は、規格書に準じて開発すること。
◆同一要項については、IEC61508に統合
機能安全規格として整合性を保つため、同一要項については1つの規格書で規定。

© 2024 Verification Technology Inc.

例：ISO26262-2018規格



© 2024 Verification Technology Inc.

全体的な安全管理への対応

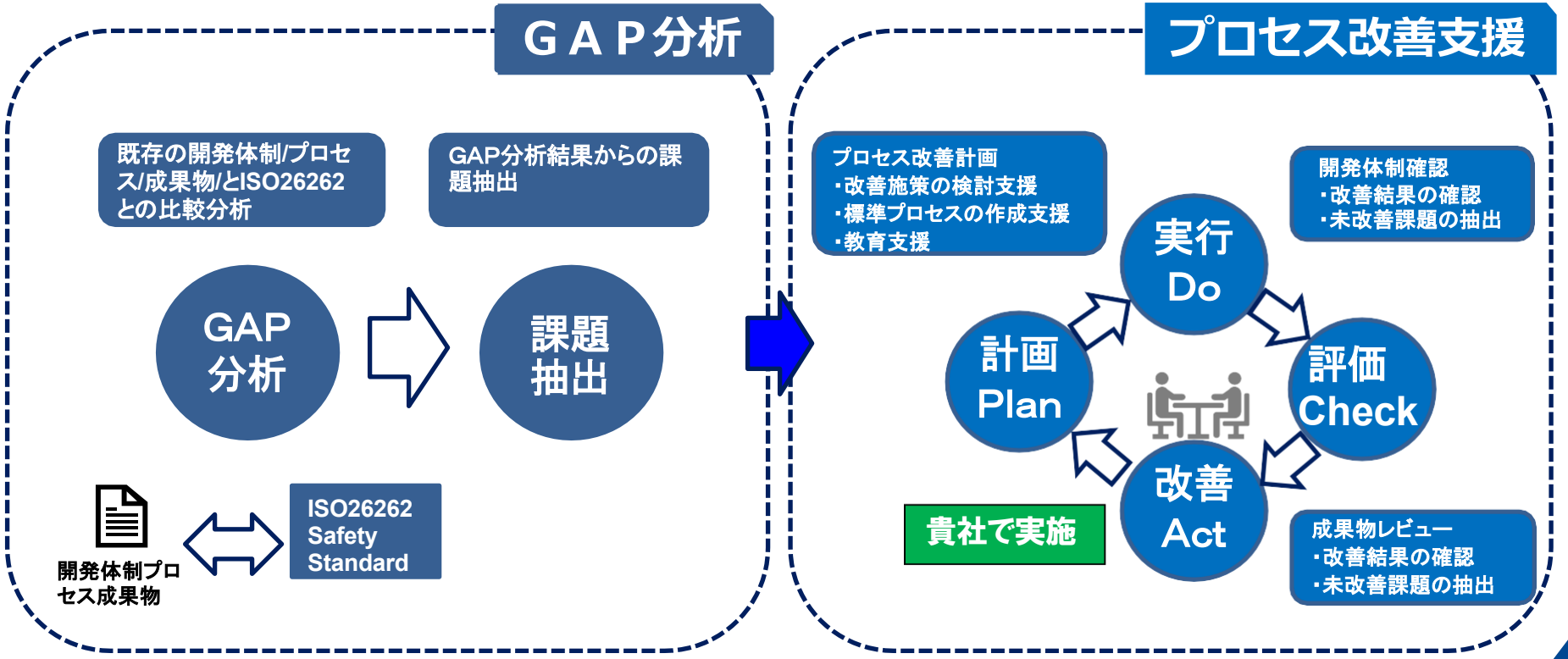
会社として/プロジェクトとしての安全規の作成

機能安全部門への対応例機能安全コンサルタント

Point！

GAP分析結果からのプロセス改善支援を行います。

【導入教育】【GAP分析】【開発プロセス構築】
GAP分析フレームワークで課題を抽出し、顧客の既存プロセスを大きく変えることなく機能安全対応を盛り込んだ製品開発の支援。顧客とともにPDCAを実施し、今後のプランを見据えた開発プロセスの構築まで支援。



© 2024 Verification Technology Inc.

開発プロジェクトへの対応例

- ISO26262の場合-

プロジェクトに参画し、一緒に
製品を開発・検証を行う

開発プロジェクトへの対応例：機能安全サービス (1/2)

Point !

コンセプトフェーズからのハードウェア機能安全開発支援

お客様がご希望する業務範囲に対して、機能安全規格観点でイタレーションが発生しないご提案と業務を実施致します。

製品コンセプト

- 機能仕様決定
- 企画要件

コンセプトフェーズ

- アイテム定義の仕様作成
- ハザード分析とリスクアセスメントの実施
- 安全計画(SP、V&V)作成
- 安全要求仕様書(SRS)作成
- 安全コンセプト(SC)の仕様策定

システム設計フェーズ

- 技術安全コンセプトの仕様策定
  (技術安全要求 / 安全機構 / システムアーキテクチャ設計仕様 / 技術安全コンセプト / 安全分析 / システマチック故障回避 / HSIの仕様等を含めて作成)

SoC Logic設計フェーズ

SoC組込みSW設計フェーズ

© 2024 Verification Technology Inc.

開発プロジェクトへの対応例：機能安全サービス (2/2)

Point !

コンセプトフェーズからのハードウェア機能安全開発支援

お客様がご希望する業務範囲に対して、機能安全規格観点でイタレーションが発生しないご提案と業務を実施致します。

SoC Logic設計フェーズ

- ハードウェア仕様作成
  (ハードウェアアーキテクチャの設計 / ハードウェア安全要求の仕様策定 / 機能安全機構の仕様策定)
- 安全分析(FMEA / FTA / FMEDA)
- 機能仕様書・実装仕様書作成
- ハードウェア設計
  (機能部・安全機構部のコーディング)

SoC組込みSW設計フェーズ

- ソフトウェア仕様作成
  (ソフトウェアアーキテクチャの設計 / ソフトウェア安全要求の仕様策定 / 機能安全機構の仕様策定/従属故障分析と報告書作成)
- 安全分析(FMEA / FTA)
- ・実装仕様書作成
- ソフトウェ機能仕様書アユニット設計＆実装
  (機能部・安全機構部のコーディング)

SoC Logic検証フェーズ

- 検証仕様作成
- 検証項目リスト作成
  (Fault Functional Simulation用 / Fault Injection Test用)
- 検証環境作成
- ブロック検証
- 全体検証
- 検証結果報告書作成
  (HWアーキテクチャメトリックの評価)

SoC組込みSW検証フェーズ

- 検証仕様作成
- 検証項目リスト作成
  (Fault Functional Simulation用 / Fault Injection Test用 ,カバレッジメトリック込)
- コード分析(コードレビュー)
- 検証環境作成
- ソフトウェアユニット検証
- ソフトウェア統合及び検証
- 組込みソフトウェアのテスト(ハードウェアインザループ等)
- 検証結果報告書作成

(SoC)システム検証フェーズ

© 2024 Verification Technology Inc.

LSI開発における機能安全実績

会社として/プロジェクトとしての安全規格の作成

Vtechの実績(1/5)

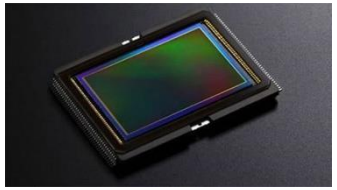
Point！　Vtechは、豊富な実績があります

①IEC61508対応の産業用ロボット用FPGA開発　　SIL-2

-IEC61508の導入サポート
-技法の解説書及びチェックリスト作成
-システムの分析結果に基づいたアーキテクチャ仕様書及び設計仕様書作成
-設計、検証及びFPGAデータ作成
　　モニター回路の組込み及びカバレッジの算出

②ISO26262対応のイメージセンサー開発　　ASIL-B(D)

-安全分析
-安全設計及びSafety Mechanismの要求仕様作成
-Safety Mechanismを含む設計、検証



③ISO26262対応の次世代ヘッドライトシステム開発　　ASIL-B

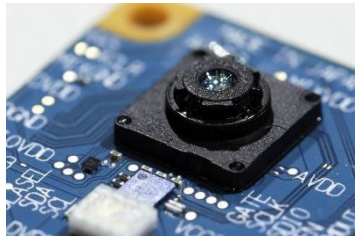
-開発部門と品質部門に対してISO26262導入サポート
-安全分析
-安全設計及びSafety Mechanismの要求仕様作成
-Safety Mechanismを含む設計、検証
-開発メンバーの機能安全トレーニング

© 2024 Verification Technology Inc.

Vtechの実績(2/5)

④ISO26262対応のTOFセンサー開発　　ASIL-B(D)

-安全分析
-安全設計及びSafety Mechanismの要求仕様作成
-Safety Mechanismを含む設計、検証



⑤ISO26262　　機能安全マネージメント業務

-Configuration Management Leader
-Document Management Leader
-Reqtifyを使用したトレーサビリティ検証
-顧客のSafety Managerの元、支援プロセス全般を実施

⑥Fault insert simulatorのベンチマークテスト

-EDA2社のFault insert simulatorのベンチマークテスト
-標準環境作成
-手順書作成
-ベンチマークレポート結果に基づき、購入ツールを決定、その後の実運用も担当

※EUでは2025年にインキャビンに対してISO26262の対応が必須になります。

© 2024 Verification Technology Inc.

Vtechの実績(3/5)

⑦標準開発プロセスの改善コンサルティング

-標準プロセス改善コンサルティング
-標準規定改訂コンサルティング
-標準手順書改訂コンサルティング
-規格の記載内容を解釈し、解釈に基づいて顧客の開発プロセスの改善と標準規定類の改訂コンサルティング

⑧ISO26262対応MCU開発コンサルティング　　(ASIL-B)

-コンセプトフェーズ(アイテム定義/HARA/機能安全コンセプト)のコンサルティング
-システムフェーズ(技術安全要求仕様/技術安全コンセプト等)のコンサルティング
-初回開発品種のコンセプトフェーズ及びシステムフェーズのコンサルティングを実施。今後の開発品種のベース構築。

⑨ISO26262対応テンプレート/ガイドライン整備

-Part2からPart10の成果物に対応する**規格対応テンプレート整備**
-規格対応ドキュメント作成時の**ガイドライン整備**

© 2024 Verification Technology Inc.

Vtechの実績(4/5)

⑩ISO26262開発プロセスの立ち上げコンサルティング

-GAP分析
-標準プロセス/体制立ち上げ
-開発フロー立上げ
-テンプレート/ガイドライン整備
規格の記載内容を解釈し、解釈に基づいて顧客の標準規定類や、開発プロセスについてコンサルティング

⑪IEC61508開発プロセスの立ち上げコンサルティング

-GAP分析
-標準プロセス/体制立ち上げ
-開発フロー立上げ
-テンプレート/ガイドライン整備
規格の記載内容を解釈し、解釈に基づいて顧客の標準規定類や、開発プロセスについてコンサルティング等

© 2024 Verification Technology Inc.

Vtechの実績(5/5)

⑫ISO13849対応テンプレート/ガイドライン整備

-Part1 ， Part2の成果物に対応する規格対応テンプレート整備
-規格対応ドキュメント作成時のガイドライン整備
規格の記載内容を解釈し、解釈に基づいて顧客の標準規定類や、開発プロセスについてコンサルティング

⑬ISO13849 SRS作成サポート(PL a / PL b)

顧客仕様と規格に基づいて、安全機能の仕様化と要求仕様作成をサポート

⑭各種機能安全セミナー

顧客の要望/状況に合わせた各種セミナーを実施
-ISO26262(基礎編)
-ISO26262(エンジニアリング編)
-ISO26262(機能安全管理者編)
-IEC61508 (基礎編)
等

© 2024 Verification Technology Inc.

まとめ

- 当社はLSI開発における安全を担保する会社です
- LSIのアーキテクチャを熟知したエンジニアがFSE、FSMの資格を保有しています
- 柔軟な体制作りから各種機能安全開発にお応えします
- 機能安全における

導入⇒安全分析⇒安全設計⇒検証までを一気通貫で

お任せください

© 2024 Verification Technology Inc.

Thank you!

ベリフィケーションテクノロジー株式会社
■本 社
〒222-0033 横浜市港北区新横浜2-3-12 新横浜スクエアビル5F
TEL：045-470-8310　FAX：045-470-8319
□関西支社
〒600-8813 京都府京都市下京区中堂寺南町134 KRP2号館2階
TEL：075-950-0430　FAX：075-950-0431