Business Cube & Partners

SEooCとしての電動化システム　安全論証のポイントと事例紹介

ビジネスキューブ・アンド・パートナーズ株式会社

本日のアジェンダ

Business Cube & Partners

- 会社紹介(Biz3)
- SEooC活用のモチベーション
- SEooCの安全論証ポイント
- 事例発表(株式会社ケーヒン様)
  - 会社紹介
  - 事例発表
- まとめ

本日のアジェンダ

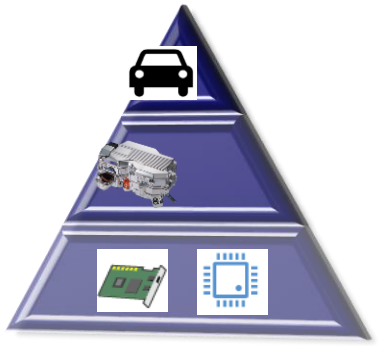
- 会社紹介(Biz3)
- SEooC活用のモチベーション
- SEooCの安全活動と論証ポイント
- 事例発表(株式会社ケーヒン様)
  - 会社紹介
  - 事例発表
- まとめ

100年に一度の変革期

Business Cube & Partners

構造の変化

系列　垂直統合
インテグラル型アーキテクチャ



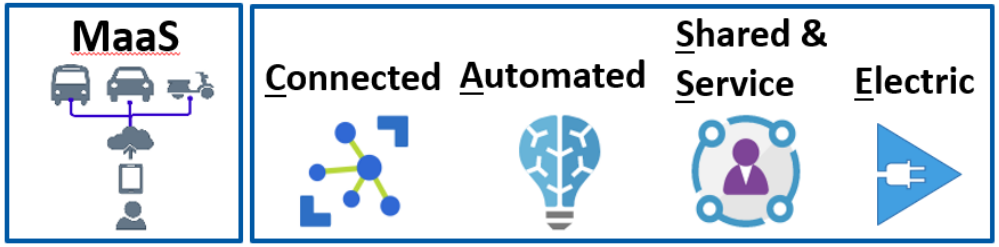
水平分業　アンサンブル
モジュラー型アーキテクチャ

垂直統合型で築き上げられた高品質は
維持しながらモジュール統合

統合が容易にできるシステムアーキと標準的キーデバイス開発が今後のカギ

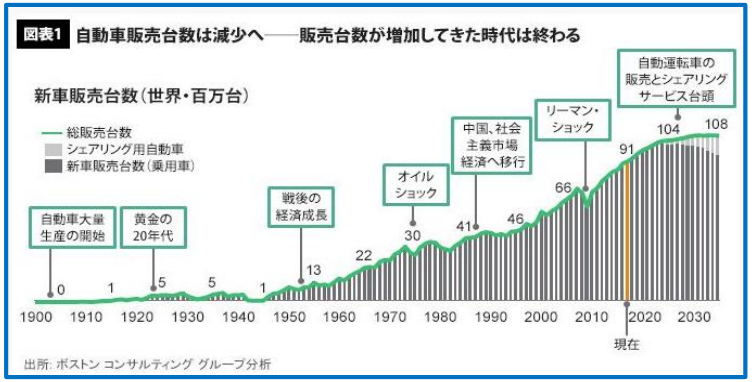
ドライバー

新しいトレンド



コアビジネス、収益構造のあり方を模索していく中での役割の変化
サービスプロバイダ、インテグレータ、キーデバイスプロバイダ、・・・

成長の鈍化



系列を超えた拡販によるコスト低減、効率化

COTS、SEooC利用のモチベーション

- **いち早く研究開発する・製品を投入する**
- **開発費を縮小する**
  - なるべく開発しない
    - 再利用して、統合する
    - 再利用できるものを開発する

- ただし下記特性を満足する必要がある
  - **安全である**
  - **セキュアである**

PERFORCE, 2019 State of Automotive Software Development Survey Resultsより引用

OSS活用に関する業界動向

- Linux Foundation
  - Automotive Grade Linux

    コネクテッドカー向けのOSSスタックの開発と採用を促進するオープンソース共同開発プロジェクト、インフォテイメント→ADAS、ADへ
  - ELISA(Enabling Linux In Safety Applications)

    Linuxベースのセーフティクリティカルシステムを構築、認証するために、共通のツールセットやプロセスを定義・保守するプロジェクト

    2019年2月から活動開始、AGLもプロジェクトに参加

The Linux Foundationの戦略プログラム担当シニア ディレクターであるKate Stewartは、次のように述べています。「エネルギー、医療、自動車など、あらゆる主要産業は、セーフティクリティカル アプリケーションにLinuxを使いたいと思っています。なぜならLinuxを使えば、製品の市場投入を早めることができ、重大な設計エラーのリスクも減らせるからです。問題は、Linuxベースのシステムが必須の安全要件を満たしていることを証明する明確な文書やツールが不足していることです。これを解決するために行われた過去の試みには、一般的に認められるような方法論を確立できるクリティカル マスが欠けていました。しかしELISAが結成されたことにより、その取り組みの実現に必要な広範なLinux Foundationコミュニティのインフラやサポートを利用することができます。」

※出典：LinuxFoundationニュースルーム記事より

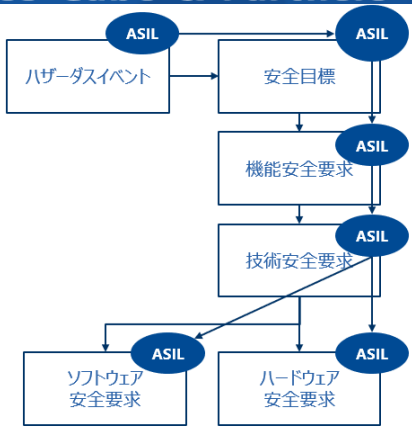
セーフティクリティカルシステムへのOSS活用にはまだ課題あり

前述の変革・モチベーションが自動車業界に留まらないムーブメントに

本日のアジェンダ

- 会社紹介(Biz3)
- SEooC活用のモチベーション
- **SEooCの安全論証ポイント**
- 事例発表(株式会社ケーヒン様)
  - 会社紹介
  - 事例発表
- まとめ

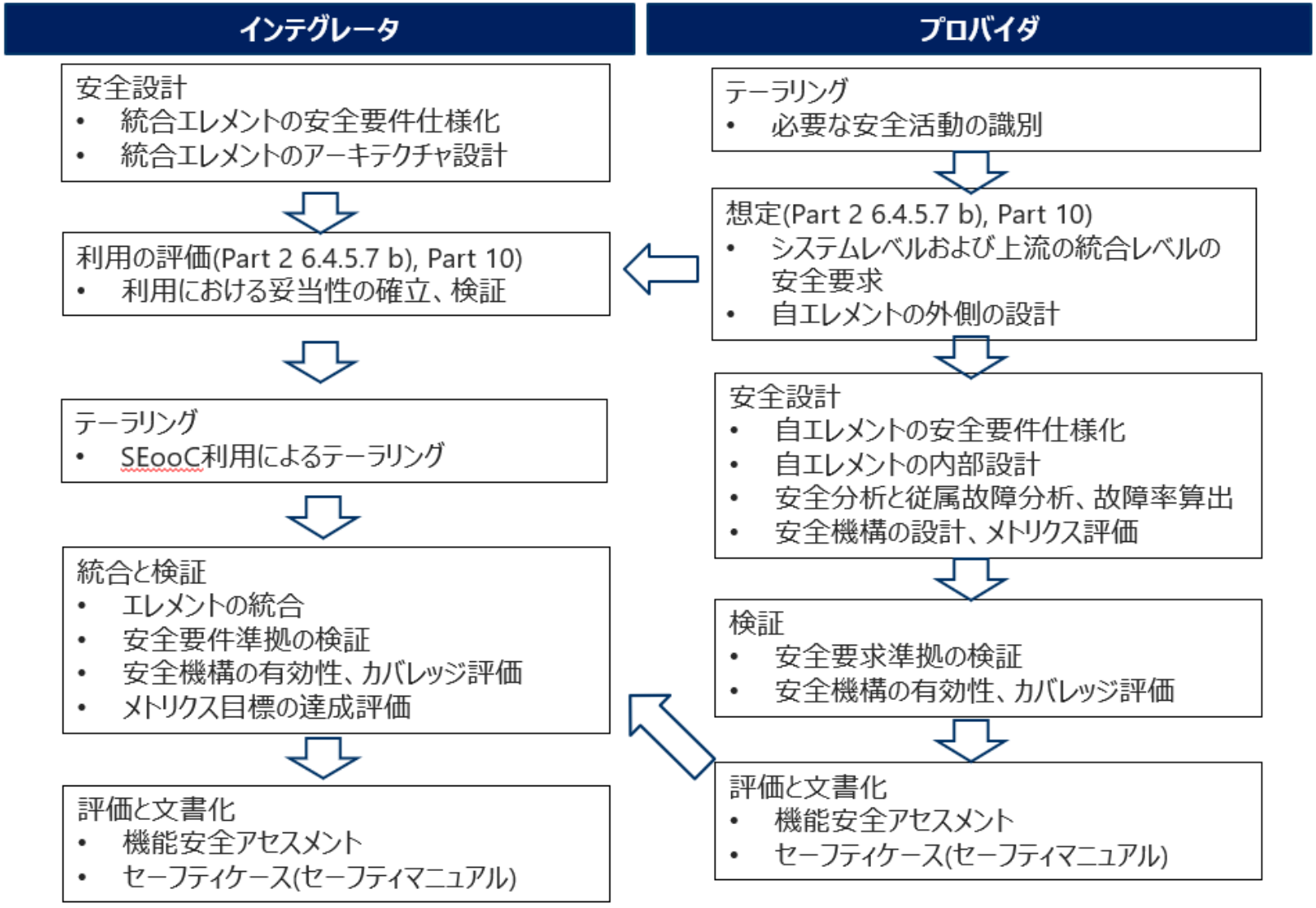
SEooC



- Safety Element out of Context
  - 背景によらない安全関連エレメント
- Context：背景とは？
  - エレメントがどのような外部環境、ユースケースシナリオにおいて使用されるか？
  - 特定の要求を受けてエレメントを開発　in Context
  - 使用用途、要求を想定して汎用的エレメントを開発 out of Context
- ISO 26262:2018
  - SEooC開発時の役割が明確化
    - インテグレータ：SEooCの利用可否判断、統合、評価
    - プロバイダ：上位システムの想定、想定に基づくSEooCの開発、情報提供

SEooC開発

Business Cube & Partners



SEooC開発における課題

- 顧客とサプライヤ間で起こるアンマッチ、ミスコミュニケーション
  - 上位システムの安全要求が実現できない
    - 例) SEooCの内部故障が統合システムで認識できない
  - 安全要求の実装不整合
    - 例) 安全機構 「外側の実装」 vs 「SEooC内部の実装」 アンマッチ
  - 要求ASILとASIL対応能力が乖離している

安全の文脈で許容できない場合は**サプライヤ側あるいは顧客側の変更が必要**

サプライヤにとって**不特定多数のアプリケーションにマッチするエレメントの開発はチャレンジ**

利用環境？ハザーダスイベント？ハザードの程度？

開発のポイント

- SEooC統合を前提とした**製品コンセプト、アーキテクチャ、プロセス**を考慮
- **モジュラーデザイン**の適用　コアデザイン＋可変点(オプション、バリアント化)
- **本質的安全設計**を考慮(故障しても安全側に倒れ、外部へ影響させない)
- **標準化にのる**、標準化する

安全論証のポイント

Business Cube & Partners

顧客とサプライヤとで主張
ミスコミュニケーションをなくす

サプライヤが主張
セーフティケースで主張

根拠
- コンテキストが想定でカバーされている
- ASIL対応能力が証明されている
- 統合状態で安全性評価されている

主張
SEooCがアイテムのコンテキストで安全に稼働する

顧客が主張
セーフティケースで主張

論拠
ISO 26262-10:2018　Clause9
- SEooCは想定に基づいて開発される
- 統合の過程で、その想定の妥当性が確立される

ミスコミュニケーションをなくす

Business Cube & Partners

- セーフティマニュアルに基づいて妥当性を議論する
  - 機能の定義
    - 機能定義、性能、外部からの利用方法
  - 機能失陥の影響
    - 前提条件　使用環境(熱、振動、作動時間、供給電圧、周りのシステムなど)
    - 故障モードとその影響範囲
  - 安全コンセプト
    - 故障影響に対しての上位レベルの安全要求
    - 安全要求から導出されるSEooC内外含めた安全機構の想定
  - 安全機構の有効性・妥当性(安全要求の準拠性)
    - 要因に対する対策の網羅性
    - 対策の有効性、妥当性
      - 評価方法、テストケースとその結果
      - メトリクス評価

使い方、ミスユースで考慮すべきハザードが変わってきます

使用環境、ミッションプロファイルの違いで評価結果(定量評価やテスト結果)に影響がでます

システム間相互作用にハザード要因が潜みます

上位レベルの安全コンセプトを考慮しないと安全要件が実現できないことがあります

テスト範囲を明確にしないと統合テストで抜け漏れます

故障率ソースの違いでメトリクスが大きく変わります

本日のアジェンダ

- 会社紹介(Biz3)
- SEooC活用のモチベーション
- SEooCの安全論証ポイント
- 事例発表(株式会社ケーヒン様)
  - 会社紹介
  - 事例発表
- まとめ

本日のアジェンダ

- 会社紹介(Biz3)
- SEooC活用のモチベーション
- SEooCの安全論証ポイント
- 事例発表(株式会社ケーヒン様)
  - 会社紹介
  - 事例発表
- まとめ

活動の背景

- システムサプライヤとしての自立
  - 背景
    - 特定OEMとの共同開発を完了し、拡販へ
    - OEMがSSR・HSR導出まで担当、ケーヒンが安全要求に基づきHW、SW開発を担当
  - 本活動への期待値
    - システムの安全性を論理的に説明可能になる

課題抽出

Business Cube & Partners

目標

- システムサプライヤとしての自立
  - 製品の安全論証ができる
  - 他OEMへ拡販できる製品の開発

現状

- 安全活動に時間がかかる、手戻りが発生
- 安全活動のフロントローディングができていない
- 機能安全プロセス通り(時間軸)の開発ができない
- システム内部の設計に理解できていないところがある

課題

- 上流の要求なしでも標準仕様が開発できる
  - **SEooCの想定の開発**
- OEMとのミスコミュニケーションをなくす仕組みを構築する
  - **セーフティマニュアルの開発**
  - **モデル記述により説明性、理解性の向上**

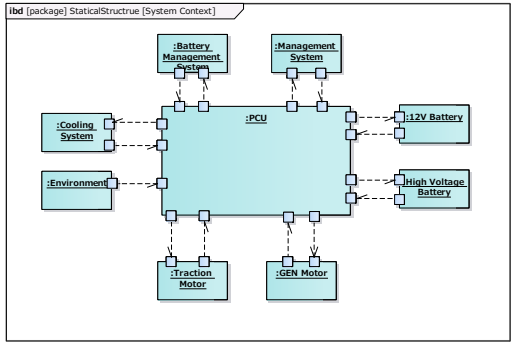
原因

- **上位の安全要求やコンセプト、設計がわからない**
- **要求がでてこないと対応できない**
- 安全設計者が不足(特定の人だけが対応できる)
- **要求事項の解釈が違い、OEMとのやり取りが多くなってしまう**
- 開発後期の仕様変更が多い
- OEM担当の設計領域に踏み込めていない

想定の導出過程

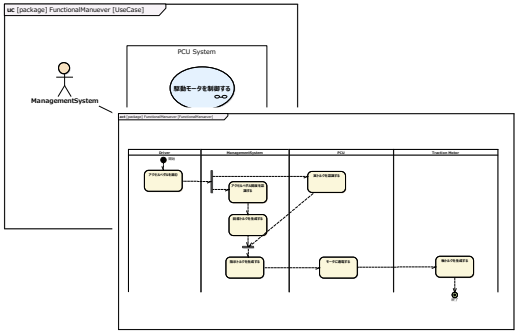
Business Cube & Partners

システムコンテキスト分析



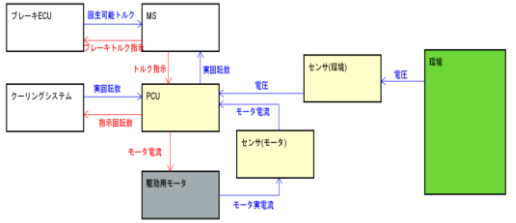
使用環境、影響の授受の想定

ユースケース分析



機能、ユースケースシナリオ、性能定義

制御構造分析



※JASPAR機能安全WG　CSテンプレートを利用

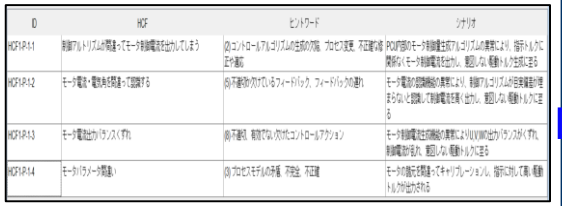
ふるまい、相互作用の定義

故障影響分析(UCA)

システム機能Failureが、SAE　J2980のハザード要因になるならない　からUCAを同定

ハザード定義とUCAの同定

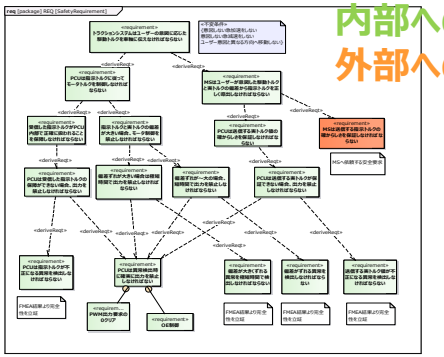
要因分析(HCF)



ヒントワードからHCFを同定

UCA要因の分析

安全コンセプト



内部への安全要求
外部への安全要求

安全コンセプトの定義

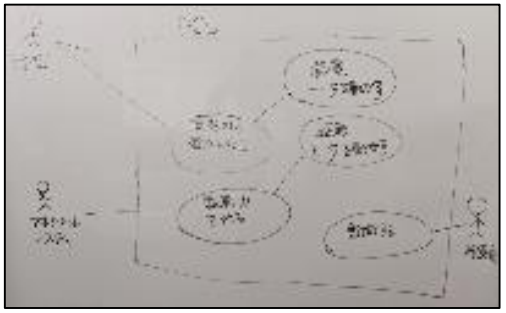
コンテキストとの創発特性に着目するためSTPAを適用

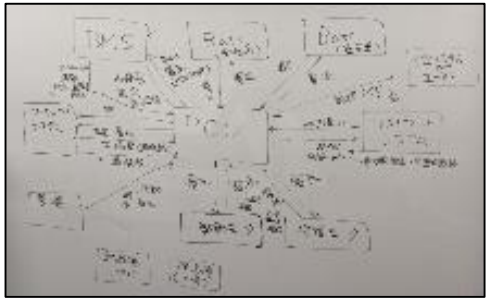
活動内容(1)

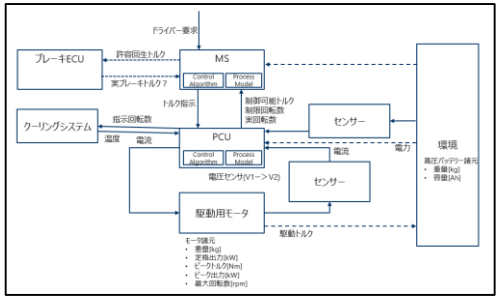
Business Cube & Partners

- 本活動の結果

開発メンバーによるコンテキストに対する議論







ユースケース分析　システムコンテキスト分析　制御構造分析

本活動による気付き

PCU開発中はお客様よりPCUの要求事項をいただき、要求仕様に対するPCU仕様を
中心に議論していたため、PCUの中身についてはお互いの認識に大きな違いはなかった。

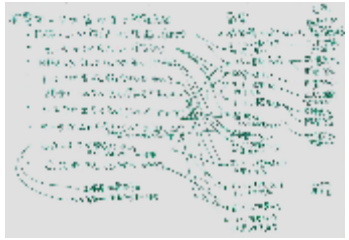
車両システムとしてPCUの外側（他システム）を意識して
議論をしたところ個々の認識に違いがある事がわかった。

今回、図示しながら議論することで、認識違いを改め、共通の認識とすることができた。

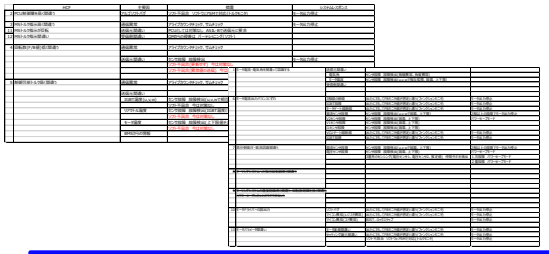
活動内容(2)

Business Cube & Partners

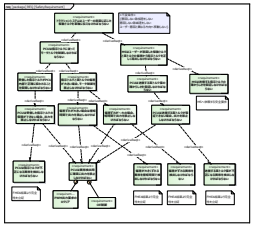
本活動の結果



ハザード分析



要因分析(UCA・HCF)



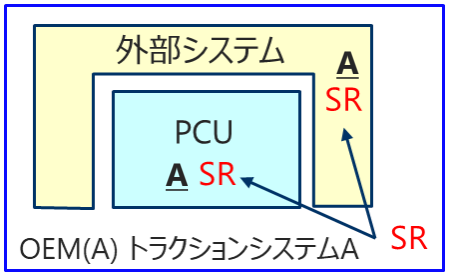
対策

本活動の結果

今回の活動を通して、OEMに対しPCUの安全性能を説明し、
安全要求提案することがシステム全体の安全につながることがわかった。

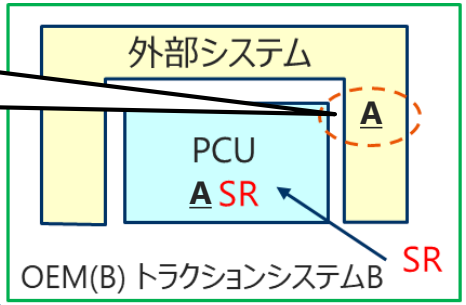
OEM(A)　システムのSR
・外部システム
・PCU

システム全体で
安全を担保する



上位レベルの安全コンセプトを考慮しないと安全要件が実現できない箇所

サプライヤより
安全提案すべき箇所



OEM(B)　システムのSR
・PCU

PCUが安全を担保すると
考えている

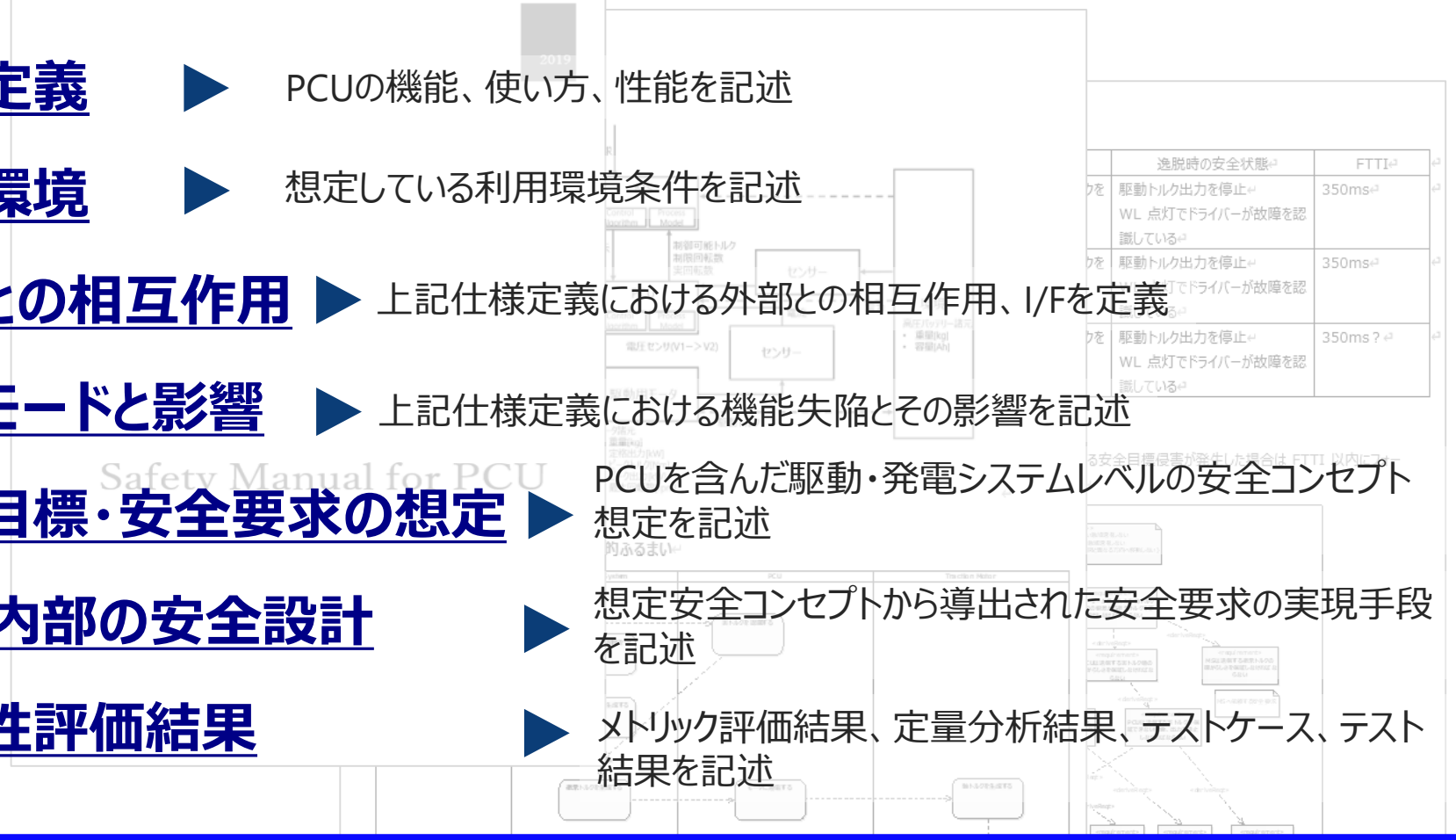
PCUはトラクションシステム「A」を前提として開発されているアイテムである事をOEMBへ説明し、外部システムに安全要求してもらう事を提案

安全提案することで、OEMとのミスコミュニケーションがなくなることがわかった。

セーフティマニュアル目次

Business Cube & Partners

1. **機能定義** ▶ PCUの機能、使い方、性能を記述
2. **使用環境** ▶ 想定している利用環境条件を記述
3. **外部との相互作用** ▶ 上記仕様定義における外部との相互作用、I/Fを定義
4. **故障モードと影響** ▶ 上記仕様定義における機能失陥とその影響を記述
5. **安全目標・安全要求の想定** ▶ PCUを含んだ駆動・発電システムレベルの安全コンセプト想定を記述
6. **PCU内部の安全設計** ▶ 想定安全コンセプトから導出された安全要求の実現手段を記述
7. **安全性評価結果** ▶ メトリック評価結果、定量分析結果、テストケース、テスト結果を記述



ケーヒン製PCUはOEMニーズにマッチし、安全性が確証できる。
OEMとのミスコミュニケーションがなくなる

セーフティマニュアル目次

Business Cube & Partners

前述から導出したセーフティマニュアル目次

・PCU機能の定義	・・・PCUの使われ方を判断してもらうため。
・使用環境	・・・規定された能力を活用してもらうため。
・外部との相互作用	・・・外部相互作用および接続I/Fを把握してもらうため。
・故障モードと影響	・・・システム仕様における想定される機能失陥と その影響を把握してもらうため。
・安全目標・安全要求の想定	・・・E/Eシステムの構成要素の機能不全に起因する安全目標侵害時の FTTIおよび安全性能とその対応を把握してもらうため。
・PCU内部の安全設計	・・・PCU内部の機能失陥で想定される故障要因に対し、 セーフティメカニズムによる安全設計を把握してもらうため。
・評価結果	・・・前述したPCUの信頼性を保証するため以下を記載する。 安全要求の実装状況、安全方策の実施状況、メトリック評価結果 定量分析結果、テストケース、テスト結果

ケーヒン製PCUはOEMニーズにマッチし、安全性が確証できる。
OEMとのミスコミュニケーションがなくなる

Business Cube & Partners

お問合せは下記までお気軽にご連絡ください。

ビジネスキューブ・アンド・パートナーズ株式会社
コンサルティング事業部
consulting@biz3.co.jp
http://biz3.co.jp