機能安全エンジニアリング　課題解決支援サービス

～安全活動、管理が実践できるようになるためのとりかかり～

Business Cube & Partners

難しさ

- ISO 26262規格理解の難しさ
  - ベースとなる安全工学に関して規格では触れていない(安全エンジニアの基礎知識として当たり前？)
  - 要求事項が抽象的　＝＞　第2版では解説が追加されて読みやすくなっているけれど
  - どこまでやるべきか、相場観が分からない　＝＞State of the artsは存在
  - 自分の役割・立場に応じて規格の必要な箇所を理解しなければならない
- 座学トレーニングの難しさ
  - 規格の範囲が広い、役割の違い、等で受講者の学習ニーズと合わせにくい
  - どこまでやったらよいか具体例を伝えづらい(大げさに書くと訴訟リスクも存在)
- 座学ベースで機能安全活動が実践できるようになるのは難しい
  - Knowledge　≠　Capability
  - 学習の順番は重要、提供されている教育も限定的
  - 実践から得られる知見、スキルは大きい
  - 相場感の習得(業界動向やState of the artsの情報収集)

機能安全対応における不変的課題

- 安全の基礎を理解し、産業の潮流に合わせて応用できる安全エンジニアの育成
  - 基礎：安全に対する理念・倫理、安全工学知識、安全活動実践スキル
  - 応用：ISO 26262対応、SOTIF対応、新しい安全技術

- 安全エンジニア、マネージャを中心とした継続的改善活動と説明性の向上
  - リスク、リスク許容レベルは時代とともに変化
  - 要件ベースの開発も、プロセスアプローチも現代車載システム開発では当然のこと、本当の難しさは説明性あるセーフティケースを作り上げること

安全エンジニア・マネージャ候補の方に寄り添って、実践できるまでの近道を示し、機能安全に関する課題解決に向かいたい

機能安全エンジニアリング　課題解決支援サービスのご紹介

Business Cube & Partners

機能安全エンジニアリング　課題解決支援サービス　フレームワーク

Business Cube & Partners

General	Specific

機能安全エンジニアリング実践支援コース

ここから始める機能安全トレーニング(6h)

これから機能安全対応を始めるにあたり、どこからとりかかればよいかのコツを学ぶ

機能安全スキルアップトレーニング エンジニアリング編(6h)

安全エンジニアが、「とりかかり」を現場で実践するための手法を学ぶ

機能安全スキルアップトレーニング マネジメント編(6h)

安全マネージャが、「とりかかり」を現場で実践するための手法を学ぶ

機能安全実践支援ワークショップ

個社・プロジェクトが直面している課題を議題に、課題解決方法とアクティビティ化を支援

機能安全実践支援コンサルティング

プロジェクトの安全活動における課題解決をエンジニアリング、マネジメント双方の視点で支援

規格解説型トレーニング

ISO 26262 規格内容を理解する
※オンサイトトレーニングでの提供

セーフティエンジニアリング理解度・習熟度

ここから始める機能安全トレーニング

- これから安全活動にとりかかる、実践してみて手が進まないお客様に対して、どこからとりかかったらよいかのポイントを解説
- 車載システムエンジニアリングの基本として、全てのエンジニアの方に有効
  - 安全に関する基礎知識
    - ISO/IECガイド51に基づく「安全の基本アプローチ」の理解
  - 安全エンジニアリングのとりかかり
    - システムを正しく理解する
    - システムの危なさを理解する
    - ソリューションを考える
  - 安全マネジメントのとりかかり
    - 安全目標を達成するための作戦を立てる
    - 監視して制御する
    - エビデンスを提供し、判断する
  - 最終点検
    - 説明してみる

機能安全スキルアップトレーニング

- 安全活動の実践にトレーニングの焦点を絞り、役割別に安全活動のポイントや安全活動の具体的手段を解説、トレーニング後に自社で安全活動実践に取り掛かれる知識を提供
- エンジニアリング編（セーフティエンジニア向け）
  - 実践的な安全設計およびテスト実施のコツ
    - システム分析手法
    - 安全設計手法
    - 安全分析手法
    - 事例で考える安全コンセプト、安全機構と安全方策
- マネジメント編（セーフティマネージャー向け）
  - 実践的な安全計画および安全論証のコツ
    - 論証を念頭に置いた安全計画
    - プロセスモデルを参考にしたアプローチ
    - 安全論証手法

課題解決ワークショップ

- 個社・実プロジェクトの課題を解決するための短期集中型ワークショップ
- ワークショップ内での課題解決、または問題解決までの計画立案までをご支援
- トレーニングでは扱えない、自社の具体事例を使って議論することで、より理解度、習熟度を高める
- 事前情報として以下をご提供いただき、ワークショップ進め方を協議
  - 現状の問題点や解決したい課題
  - ワークショップへの期待値

課題解決ワークショップ事例

- 背景
  - システムサプライヤとして自立化
    - OEMがシステム、TSRまでを開発、要求を受けてHW,SWを開発するスタイルから、システムサプライヤとしてシステム開発・システム提案までを担当
    - 特定OEM向け製品開発から、製品拡販が事業部としての命題化

- 課題
  - システムの正しい理解と可視化
    - システムに求められる要求事項を把握する
    - ブラックボックスであったシステム仕様を正しく理解し、可視化する
  - システム安全性の説明
    - システムが安全であることの論理的説明が可能になる

課題解決ワークショップ事例

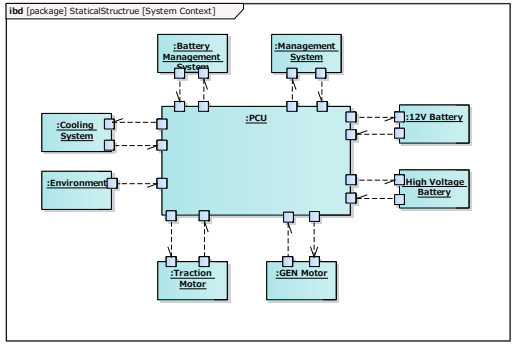
- 課題解決ワークショップ
  - 本ワークショップでは「システム安全性の論理的説明が可能になる」をメインの解決課題に設定し、以下の活動を実施。(全7回のワークショップ)
    - システムのユースケース、外部環境の影響からシステムへの要求を理解する
    - ユースケース実現のための制御構造分析を行う
    - 制御構造分析よりハザード分析実施およびハザード原因を特定する
    - ハザード低減対策を設定、安全コンセプトとしてまとめる
    - 安全コンセプトと現フェールセーフ仕様の対比を行い、網羅性を確認する
    - 上記をセーフティマニュアルとして文書化
  - 上記を適切なモデル記述し成果物化することで、理解しやすく説明性のあるエビデンスを資産化するように心掛けた
    - ユースケース図、システムコンテキスト図
    - 制御構造図
    - 安全分析モデル(STPA)
    - 要求図(安全要求)、安全コンセプト(安全機構の動的、静的アーキテクチャモデル)

課題解決ワークショップ事例

Business Cube & Partners

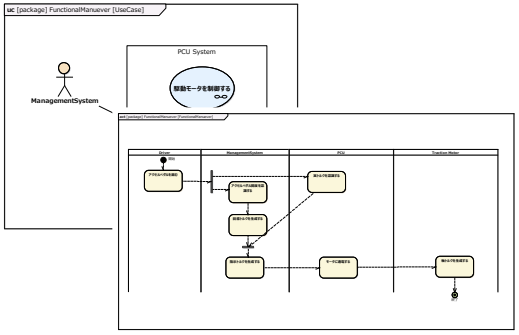
- ワークショップからの成果物例

システムコンテキスト分析



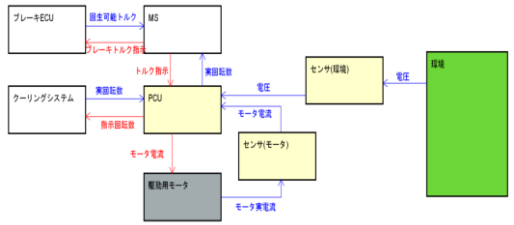
使用環境、影響の授受の想定

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

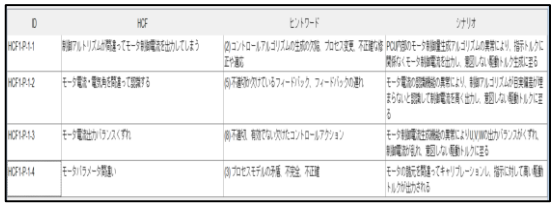
ふるまい、相互作用の定義

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

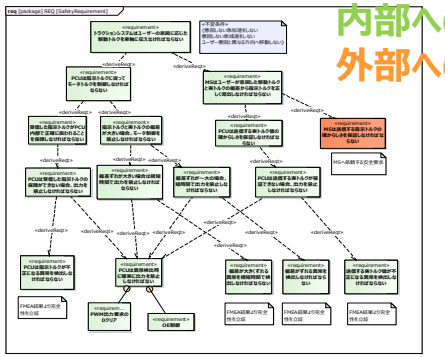
要因分析(HCF)



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

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