鉄道信号システムの安全性評価

【概要】

鉄道信号システムは、冗長構成による比較、故障診断、故障検知時の安全側固定という仕組みを積極的に組み込むことにより、フェールセーフとなる様に設計されます。

鉄道事業者やメーカが、新たに鉄道信号システムを開発した際に、作成されたドキュメントをベースに安全設計のためのアドバイスや安全性評価を実施しています。国際規格も参考にしています。

【特徴】

・「設計段階」においては、故障モードが特定され、各故障モードに対してフェールセーフを基本とした対策がほどこされていることを確認します。また、システム全体を観点とした確認のため、FTA、 FMEAも確認します。
・「試験段階」においては、入力条件、判定条件、試験結果について確認します。また、設計仕様書に対して試験項目が対応していることも確認します。

【用途】

本安全性評価は、第3者の視点での安全性評価です。評価対象文書の作成は必要となりますが、設計、製造物を再確認する機会となります。評価対象文書は、次期システム開発時のベースとして活用できます。

ハードウェア

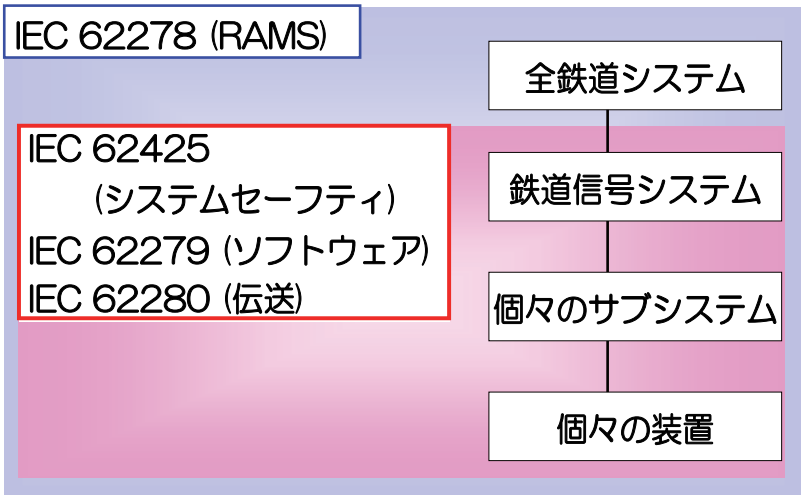
・危険側誤動作の発生頻度が従来と同等以上
・故障検出時の安全側固定
・積極的な故障診断（潜在故障の防止）
・診断回路自身の診断
・ROM・RAM診断
・入出力回路の故障診断、等

ソフトウェア

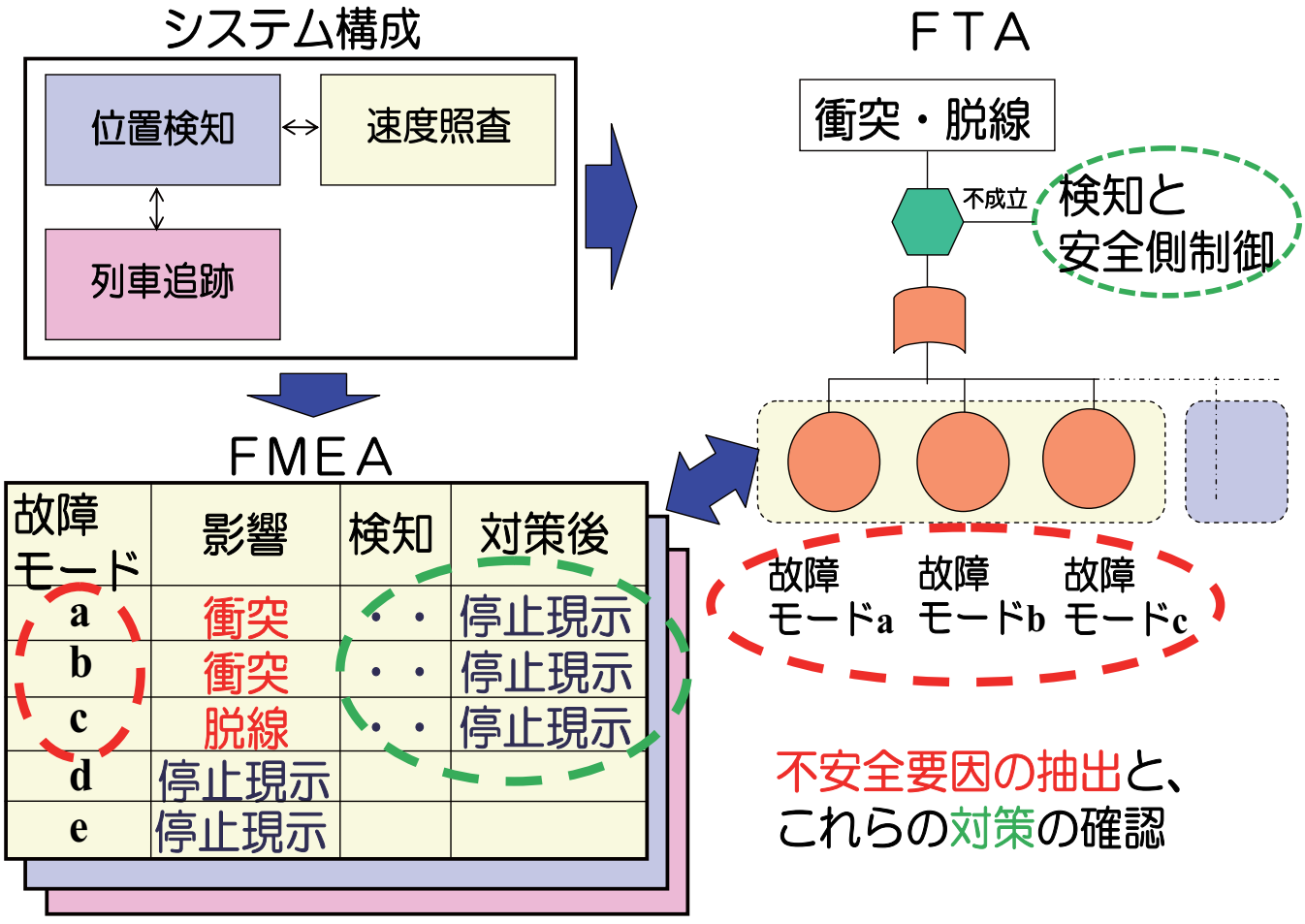
・機能仕様の明確化
・安全側と危険側の明確な区分
（プログラム構造、情報）
・実績のあるプログラム言語の使用、等

【列車保安制御システムの安全性技術指針】

安全性評価の確認項目



安全性評価に関する参考国際規格



不安全な要因の特定、対策の確認