鉄道信号システムの安全性評価

公益財団法人鉄道総合技術研究所　　信号・情報技術研究部

電気

国際規格を参考にした第三者視点の安全性評価

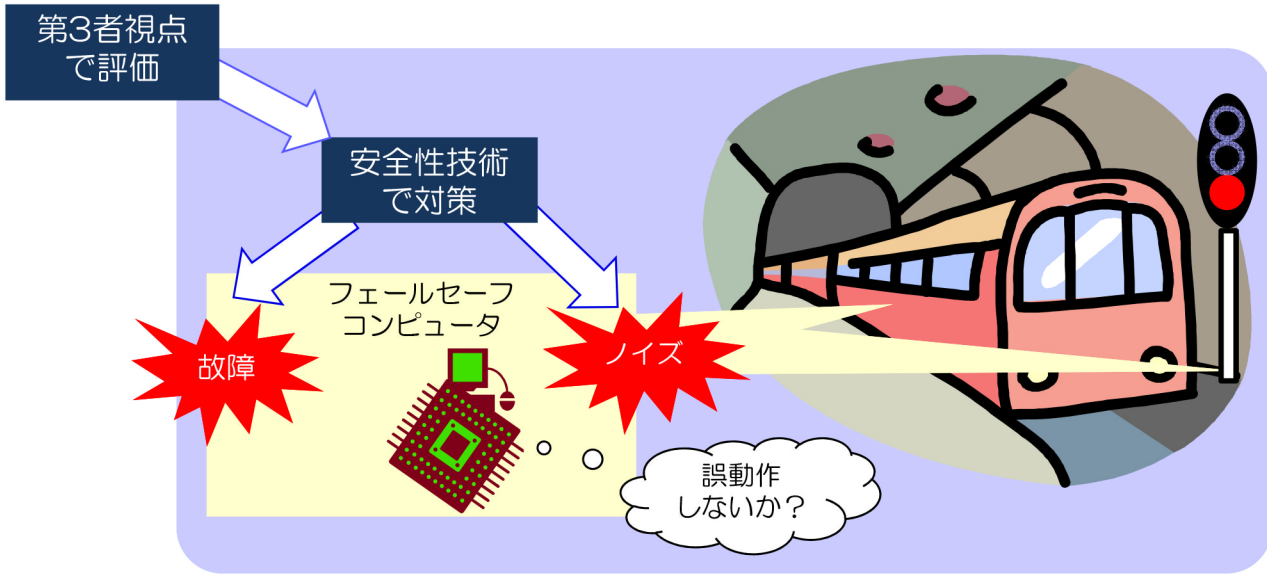
鉄道信号システムは、冗長構成による比較、故障診断、故障検知時の安全側固定という仕組みを組み込んで安全性を確保しています。鉄道総研では、新たに鉄道信号システムを開発する際に、システムの安全性確保の考え方を示す文書をベースに、安全設計のためのアドバイスや安全性評価を実施しております。

【特徴】

- 「設計段階」の評価では、システムの故障モードが特定されているか、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施されていることを確認します。システム全体を観点としたFTA、ＦＭＥＡの結果も確認します。
- 「試験段階」の評価では、試験項目の入力条件、判定条件、試験結果を確認します。また、試験項目は、設計仕様書に対応していることも確認します。

ハードウェア	ソフトウェア
・危険側誤動作の発生頻度が従来と同等以下 ・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） ・診断回路自身の判断 ・ROM、RAM診断 ・入出力回路の故障診断　など	・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　など 【列車保安制御システムの安全性技術指針】

主な確認項目



主な確認項目のイメージ