列車制御システムの設計仕様書の安全性確認手法

A Method to Verify System Requirements Specifications Based on Safety Requirements for Train Control Systems

【概要】

列車制御システムにはフェールセーフ性が求められます。近年、相互接続される機器の増加、保守性や稼働率の向上のための機能の増加等により、システムの大規模化、複雑化が進み、安全性確認に多くの労力を要します。そこで、鉄道事業者がシステム全体を把握するため、またメーカがサブシステムを設計するために必要となる、システム全体の動作を定義するシステム設計仕様書を対象とした確認手法を作成しました。

【特徴】

提案手法はシステム開発の最上流に位置するシステム設計仕様書における論理誤りや定義漏れ、複数装置間での仕様の不整合（図1）を低減します。

安全要件に関わる仕様が定義されていることを、システムを構成する機能単位で定めた安全要件のフォーマット（図2）を使用して確認し、機能間での記載内容の整合性を確認します。（図3）

安全要件のフォーマットは対策の優先順位や適用箇所を考慮して定めました。また、これら確認作業の容易化のため、支援ツールを試作しました。（図4）

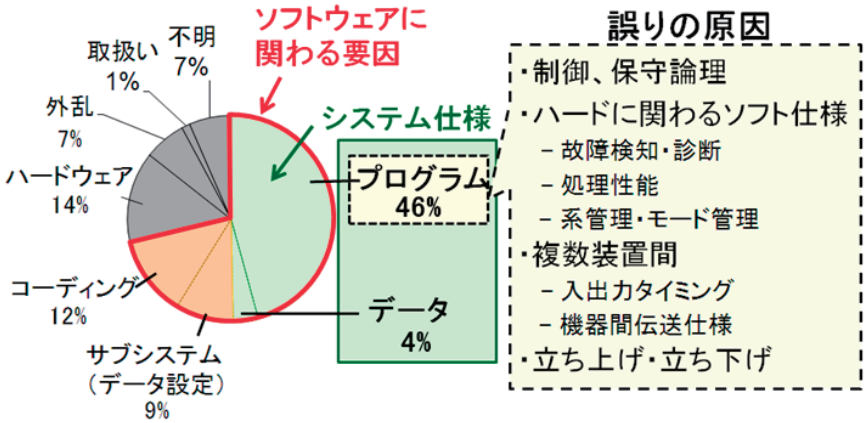

図1　電子連動端末部相当の開発段階での試験（5か月間）の障害分析結果

【用途】

列車制御システムの設計仕様書の確認を目的とし、仕様誤りの低減、新規システムの設計仕様書作成支援に役立ちます。

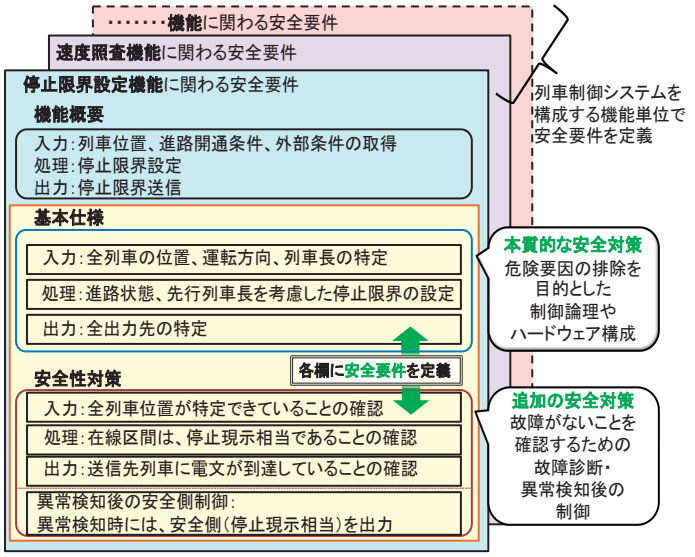

図2　安全要件のフォーマット

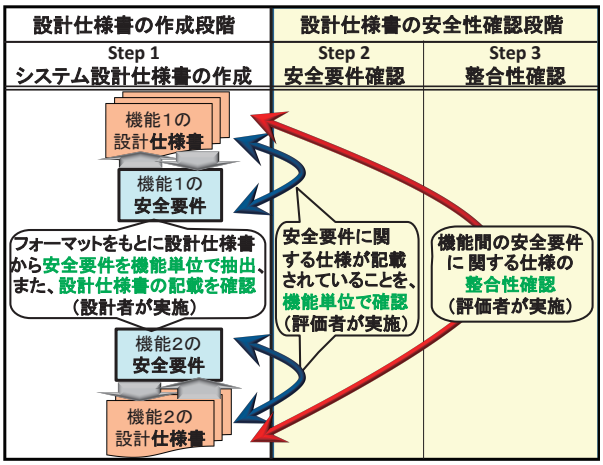

図3　安全性確認手法

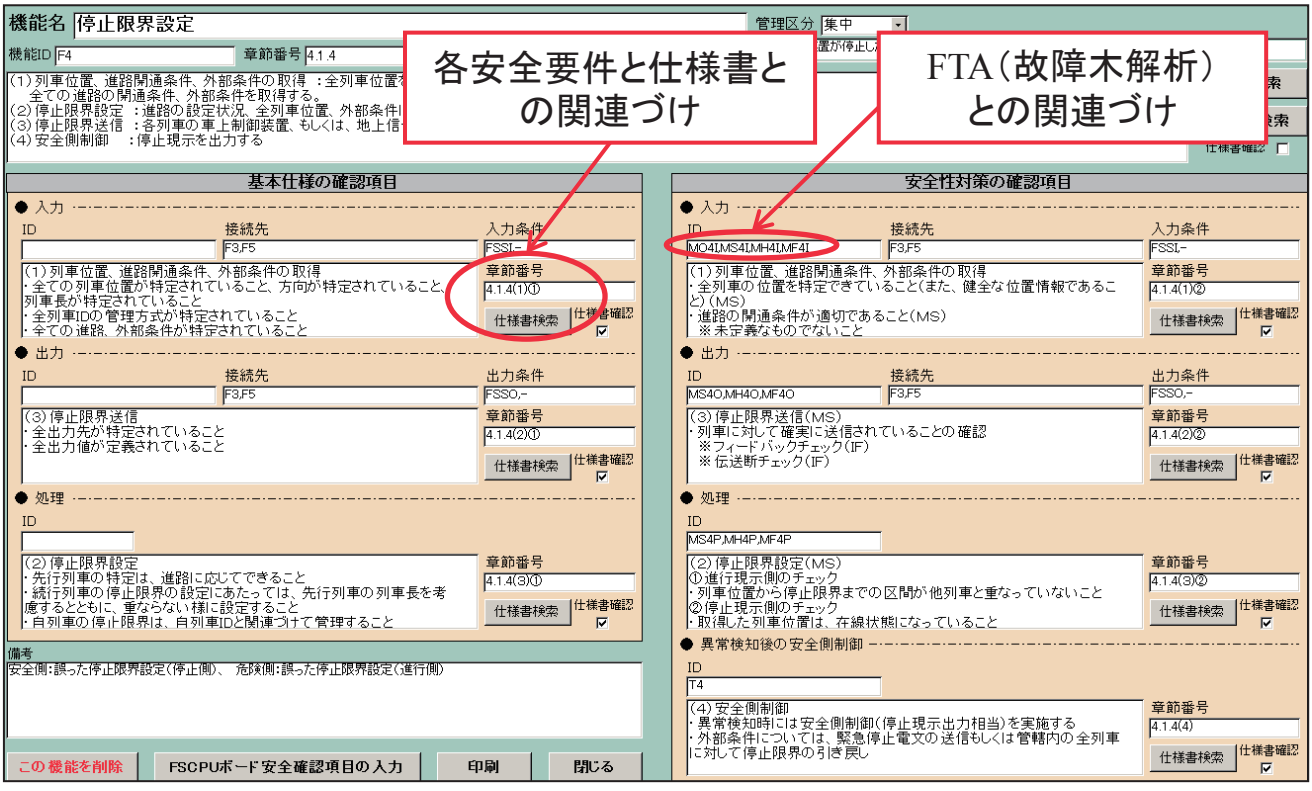

図4　安全要件の確認画面の例

特許出願中。

公益財団法人鉄道総合技術研究所
信号・情報技術研究部　列車制御