関西地区技術交流会　発表概要

信号システムの安全性評価

信号通信技術研究部（列車制御）
岩田浩司

１．はじめに

鉄道信号システムは、信頼性とともに高い安全性が要求される。この安全性レベルを維持するため、設計段階においては FTA（Fault Tree Analysis）、FMEA（Failure Mode and Effects Analysis）などの安全性解析によりシステムにおける不安全な事象を特定し、フェールセーフを基本とした安全性対策が施される。本発表では、鉄道総研で実施している信号システムの安全性評価の取り組みについて述べる。

２．鉄道信号システムの概要

電子連動装置が導入されてから２０年以上経過している[1)]。フェールセーフな CPU ボードを用いたソフトウェアで実現された機能は、CPU 処理能力の向上とともに多機能化し、保守性も向上している。装置間のネットワーク化も進み、信号機自体も端末化したネットワーク信号システムも実用化された[2)]。

また、RAMS（信頼性、可用性、保守性、安全性）国際規格（IEC62278）など、鉄道信号に関わる国際規格[3,4,5,6,7)]が制定され（図１）、鉄道信号システムの開発ライフサイクルと、システムの安全目標を表わす安全性インテグリティレベル（SIL）を意識したシステム開発もなされつつある。

近年のシステムにおける特徴としては、装置内のハードウェア、ソフトウェアそれぞれの安全性・信頼性だけでなく、これらを組み合わせた装置全体としての安全性、さらに、複数装置をネットワーク接続した信号システム全体としての安全性がより一層重要になった点があげられる。このシステムの確実な動作には、システム開発のライフサイクルにおいて最上流に位置づけられる、システム全体としての設計仕様が非常に大きな役割を担う。

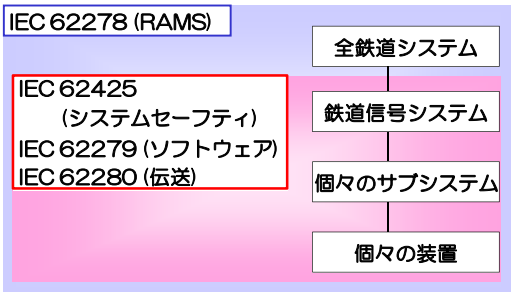

図１　鉄道信号に関わる国際規格

３．鉄道総研における安全性評価

信号システムには高い安全性が要求され、システム開発のライフサイクルの初期の段階から最終段階までの間において発生する故障・誤りを想定した安全設計が求められる。故障・誤りとしては、システム仕様の誤り、ハードウェア故障、ソフトウェア誤り、ヒューマンエラーがあげられる。これらに対して信号システムが安全であることが、システムを設計・製造した会社において十分確認されている。鉄道総研での安全性評価は、鉄道総研という第３者の新たな視点からシステムを改めて見直すことで、システムの安全性の更なる向上を目指したいというニーズにこたえるべく実施している。以下に、評価の観点から見た安全設計の主要なポイントを示す。

（１）システム内の不安全事象の特定

信号システムに内在する不安全な事象の抽出は、FTA(Fault Tree Analysis)、FMEA(Failure Mode and Effects Analysis)により、初期の設計段階から実施される。また、システム構成、FTA、FMEA 間で相互にチェックし、不安全な事象の抽出の更なる確実化がはかられる（図２）。これらの特定された不安全事象に対し、フェールセーフとなる様に表１に示す項目を基本とした安全設計が行われる。

（２）ハードウェア

半導体の集積回路は信号用リレーと異なり、装置の故障モードに非対称性がなく、故障モードの特徴に安全性を期待できない。よって、システム全体として安全を確保すべく、冗長構成による故障検知、積極的な故障診断、故障検出時における出力の安全側固定を基本とした安全設計が行われる。

例えば、フェールセーフ CPU ボードは、CPU が２台搭載され、照合回路を用いて相互に処理状態を常時チェックするとともに、メモリや入力回路などに対しても積極的に故障診断を行い、故障の潜在防止がはかられる。また、故障検出時には、安全側（赤信号側）に出力が固定される。

（３）ソフトウェア

ソフトウェアのライフサイクル例を図３に示す[4]。設計仕様は、段階が進むにつれて詳細化され、テストは各設計段階に対応したテスト仕様を定めて実施される。各段階で定めた仕様は次の段階に確実に反映することが重要である。各段階終了時における適合確認、最終的な妥当性確認においては、設計段階間のトレーサビリティ、テスト項目と設計仕様間のトレーサビリティなどが確認される。

４．おわりに

鉄道に対する社会的な安全性の要求レベルは高く、信号システムはこの安全性の確保に大きく関わる。本安全性評価業務を通し、少しでも鉄道の安全性向上に貢献できればと考える。

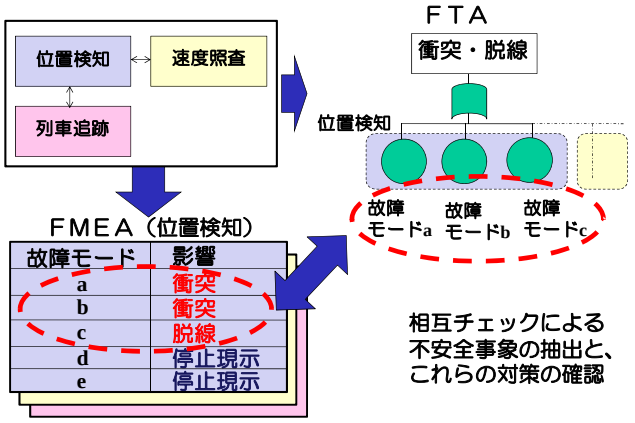

図２　不安全事象の抽出

表１　安全確保の基本条件

分類	項目
ハードウェア技術の基本条件	・危険側障害（１０万年に１回） ・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 ・入出回路の故障診断、等
ソフトウェアの安全性の基本条件	・ソフトウェアに対する要求の明確化 ・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[8]）

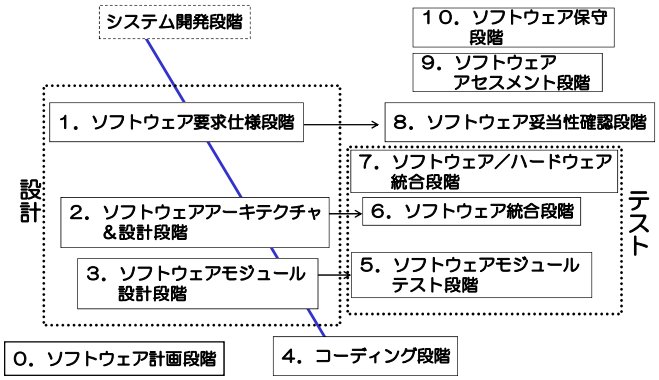

図３　ソフトウェア開発ライフサイクル

参考文献

1)秋田、渡辺、中村: 電子連動装置 SMILE の開発, 鉄道技術研究報告 No.1361, 1987

2)遠藤、国藤:　駅構内ネットワーク信号制御システムの開発, JR East Technical Review No.20, 2007

3)IEC62278 : Railway applications - Specification and demonstration of reliability, availability, maintainability and safety(RAMS), 2002

4)IEC62279 : Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems, 2002

5)IEC62280-1 : Railway applications - Communication, signalling and processing systems - Part 1 : Safety related communication in closed transmission systems, 2002

6)IEC62280-2 : Railway applications - Communication, signalling and processing systems - Part 2 : Safety related communication in open transmission systems, 2002

7)IEC62425: Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling, 2007

8) 鉄道総研: 列車保安制御システムの安全性技術指針,1996