講演 9. 改定された RAMS 関係規格の注意点について

－鉄道における国際規格 IEC 62425 規格の変更とそのポイント－

鉄道認証室　　※森　崇、吉永　純

１．はじめに　鉄道関連規格の概要

鉄道関連のシステムの海外展開に際し、国際規格との適合性が要求される場合がある。交通安全環境研究所鉄道認証室は、鉄道関連の国際規格適合性認証機関として、製品認証に関する業務を実施しており、我が国の鉄道製品海外展開の一翼を担っている。

鉄道に関係する国際規格のうち弊室が対応できる規格は、以下の通りである。

- IEC 62425[1)2)]
  鉄道信号分野における安全関連電子システムの開発と受け入れの要求事項
- IEC 62279
  鉄道の制御及び防護システムに使用されるシステムのソフトウェア開発プロセスと技術要求
- IEC 62280
  伝送システムを使用する安全関連電子システムの基本要求
- IEC 62278
  鉄道システムにおける RAMS (Reliability、Availability, Maintainability and Safety)マネジメントライフサイクルプロセスの要求

本稿においては、このうち、IEC 62425 は 2025 年 5 月に改定されたのでその注意点について述べる。なお、IEC 62278 についても 2025 年改定されている。

１．１．IEC 62425 の対象

IEC 62425 は、鉄道信号分野における開発と受け入れに主に使用されている。このうち、ソフトウェアに関する事項は IEC 62279 を参照しており、本文中は主にシステム全体と、ハードウェアの観点で規格が構成されている。

IEC 62425 は、鉄道信号分野における規格であるが、海外展開に際して、鉄道信号分野だけではなく、鉄道に使用される電子機器についての活用例も多くあり、鉄道関連国際規格の中では注目度も高い。この規格は、安全性について、「機能安全」による安全について述べているため、本稿では、まず機能安全について説明し、次に IEC 62425 規格における安全思想、また Edition 2 における変更点について述べる。

１．２．機能安全とは

安全を考える際には、「危険な状態が排除されていること。」と思いがちであるが、すべての危険な状態を排除することは一般には非常に困難である。鉄道関連規格だけではなく、一般の制御システムやリスクアセスメントにおいても、安全の定義は、“freedom from unacceptable risk”[3)]とされている。すなわち、危険な事象がないということではなく、「受け入れられないリスクがない」ことが「安全」を意味する。

次に、安全の前に「機能」がついた、「機能安全」とは

“part of the overall safety that depends on functional and physical units operating correctly in response to their inputs”

と IEC 62425 に定義されている。これを読み解くと

- 機能安全は、全体の安全の一部分である。
- 機能及び物理的なユニットが、入力に対して正常に働くことによる安全である。

ということを示しているようである。IEC 62425 については、機能安全を対象としているため、安全を実現する方法のうち、機能安全のみを議論の対象とし、また、考えられる入力に対して、受け入れられないリスクがある場合、安全とされる動作を行うということを求めている。

いうなれば、「予期された事象に対する、安全な動作の定義と実装」ともいえるわけであり、どのような危

険の原因があり、危険な原因がリスクアセスメントにおいて、受け入れられるか否かの判断を行い、受け入れられない場合は、設計時点から考えておいてシステム構築を行う方法が、機能安全であるといえる。

このような手順を踏むため、機能安全を実現するシステムにおいては、危険原因となりうるハザードの抽出、ハザードの評価、必要ならば低減対策である安全関連機能の設定、その実装が網羅的になされている必要がある。

図 1 にハザードの抽出から、安全関連機能設定までの標準的な手順を示す。

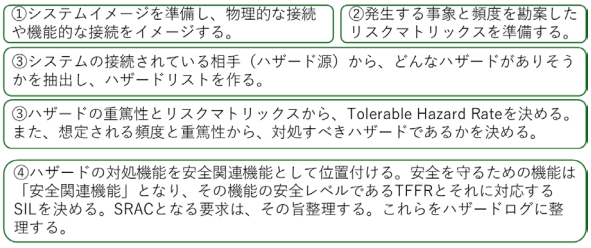

図 1　安全関連機能の設定

2．IEC 62425 における安全思想

IEC 62425 における安全性の確保は、機能安全を中心に据えられている。十分に受けいれられる安全関連機能を設定し、その機能を正しく実装することが必要である。それにはマネジメントによる安全性と、受け入れ可能とされる目標を満たしているかどうかの確率論的な安全解析に基づいたシステム設計の 2 つの大きな柱からなる。この 2 つについて次に述べる。

2．1．マネジメントによる安全

2．1．1．品質管理プロセスによる安全

品質管理プロセスは、どちらかというと「故障しないモノづくり」のために行われると一般的に考えられがちである。IEC 62425 5.2 章において、 “The purpose of the quality management system is to minimize the incidence of human errors and to improve process performance at each stage of the life cycle, and thus to reduce the risk of systematic faults.”とされており、ライフサイクル管理の各段階において、安全を阻害するヒューマンエラーをどのように防ぐか計画を行い、実施を確認するということに重点が置かれている。

2．1．2．安全管理プロセスによる安全

安全管理プロセスは、品質管理プロセスとは異なり、安全関連の systematic fault の残存リスクを最小化する作り込みを行うために実施される。すなわち、安全をどのように作りこむかのプロセスに重点を置き、品質管理プロセスを細分化し、システムの要求から、安全要求、設計及びその対応する試験の仕組みを構築するために安全プロセスが実施される。

- 構造化された文書体系
- 安全ライフサイクル
- 安全組織
- セーフティプランの構築
- ハザードと安全機能
- 安全に資するシステム設計
- Verification と Validation

などについて、プロセスを定義する。

2．2．安全解析に基づいたシステム設計の手法

IEC 62425 においての安全解析は、リスクアセスメントと、ハザードコントロールの 2 つの段階で実施される。

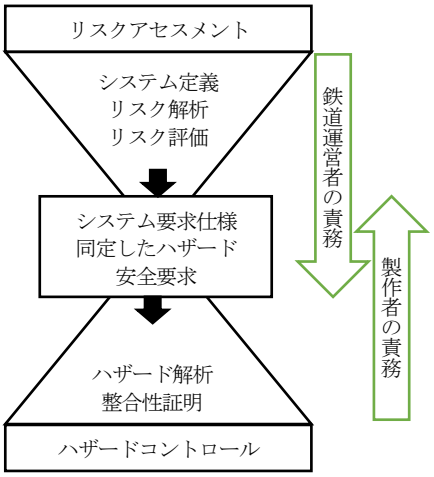

図 2　砂時計モデル

図 2 に 2 つの段階のモデルを示す。これは IEC 62425 において、砂時計モデル (The hourglass model)と呼ばれ、システムを設計するにあたり、システム定義からその安全性への整合性証明までの一連の必要な行為を示している。

まず対象とするシステムを定義し、次にリスク解析を行う。リスク解析はハザードを抽出し、そのハザードがどのような原因で引き起こされるかを解析する。

次にリスクの評価を行う。ハザード及びその原因を確認し、ハザードの重篤性及び頻度からそのリスクが受け入れ可能かどうかの判断を行う。または、ハザードの重篤性及び受け入れ基準から、基準と整合するハザードの発生頻度以下であれば受け入れ可能であるかどうかを決定する。この受け入れ可能なハザード発生頻度を Tolerable Hazard Rate (THR)という。

対策が必要とされたハザードは、システムにおいてその低減を要求するか、Safety Related Application Conditions (SRACs) として、条件を付けてハザードコントロールをするか決定する。それをシステム製作に生かしていくこととなる。

次にハザードコントロールの段階に移る。ハザードとその THR 及び安全要求をもとに、ハザードに対応する安全関連機能を設定する。

ハザードに対応する安全関連機能の失敗許容頻度を TFFR(Tolerable Functional Failure Rate)といい、THR から TFFR は導出される。もし単一の機能でハザードを防止できるのであれば、THR＝TFFR となる。

次に、TFFR を満足するような仕組みを構築する。ハードウェアの時間当たり故障頻度、故障検知時間及び故障検知率並びにメンテナンス間隔及び修理時間など、安全関連機能を維持するための必要な条件を入力し、整合性を証明することになる。

また、ヒューマンエラーなどの systematic fault は確率論による議論が難しい事項に対応するため、機能ごとの TFFR をもとに、それに応じた質の高い管理手法や開発技術を選択することにより安全性を担保する。

２．３．セーフティケースの構築

品質管理プロセス、安全管理プロセスの実施結果、そしてそのプロセスに沿って導出された技術的な安全性の証拠は、鉄道信号システムの安全性を表明する手段となりうる。鉄道信号システムの安全性は、求められる THR から、実績で十分に示すことは困難であり、プロセス管理、受け入れられるリスクの低減として確率論的な考え方とその証拠、設計の正当性、試験、確認の正当性の確認をもって表現することになる。このため、セーフティケースという図書で証拠を残し、ライフサイクル全体で管理することとなっている。

３．IEC 62425 Edition 2.0 の変更点

IEC 62425 Edition 2.0 は、2025 年 5 月に発行され、2007 年に発行された Edition 1.0 を置き換えている。変更点はほぼ技術的な改定（“This second edition cancels and replaces the first edition published in 2007. This edition constitutes a technical revision.”）であるため、マネジメントについての変更点の説明は省略する。

３．１．既存のシステムなどの取り扱い

IEC 62425 Edition 1.0 においては、規格に対応して製作を行っていない System / Subsystem / Equipment (ここでいう Equipment は、サブシステムより小さな範囲である)で、すでに受け入れられているものは対象外であるとされていた。今回 Edition 2.0 の “6 Requirements for elements following different life cycles” においてその取扱いが定まった。

- 既存の System 全体を導入する場合

既存のシステムをそのまま IEC 62425 に適合するシステムとして取り扱う場合は、安全の証拠として提示されている事項を洗い出し、適用規格との差分を解析する。また独立した安全アセスメントにより、規格に合致していることを保証する。

- 既存の Equipment を組み込む場合

既存の Equipment を組み込み、システムを構築する場合、その Equipment は規格の要求事項をすべて満たしているとは言えない場合がほとんどである。本稿では詳細には触れないが、仕様を明確にし、故障モードを明らかにすることが求められる。その上で、その故障モードが起こりえないか、故障モードを防御する機能の TFFR が満たされているか、もしくは外部装置により故障モードへの対策機能を実装することが要求される。

またシステム全体の管理として、システムの構成管理に置くこと、システムとしての Verification & Validation の対象とすることが求められる。

３．２．プログラム可能な LSI の取り扱い

IEC 62425 においては、ハードウェアの要求事項に

ついては対象とし、ソフトウェアの要求事項については IEC 62279 を適用することとなっている。しかしながら現在のシステムにおいては、そのいずれとも言い難い、LSI のロジックを回路設計者が自由に設定できる PLD(Programmable Logic Device)が普及してきており、IEC 62425 が対象とするシステムにも実装されていることが多い。

しかしながら、IEC 62425 Edition 1.0 においては、その取扱いは特に定められておらず、安全関連機能を実装する場合どのように判断をするのか明確な基準が存在しなかった。今回 Edition 2.0 において“Guidance on User Programmable Integrated Circuits”として Annex F に参考図書として要件が示された。

プログラム可能なハードウェアという観点から、Random fault(時間経過とともにランダムに故障が発生する故障)と、Systematic fault 双方を考慮する必要があることから、PLD の IEC 62425 の適用は、Random fault については通常のハードウェアと同じ考え方で対処することにより、Annex B 及び E の開発プロセスに沿い、技術的な選択は Annex E に沿うこととし、Systematic fault については、新規に追加された、Annex F を参考とするとされた。

Annex F については、ロジックを設計するための、IEC 62279 と似た管理手法だけではなく、ロジックを LSI に実装するための手法、Fail-safety を構成するための考え方、並列処理と同期に際して問題になるマイクロスタビリティ、既存のロジック設計である IP Core (Intellectual Properties Core)の活用ルールなど、この項だけで IEC 62425 のほとんどの項目が入るような内容であり、弊室としては参考になると考えている。

３．３．安全関連機能における SIL Table の定義

IEC 62425 Editon 2.0 について、Edition 1.0 からの最も目立つ変更は安全関連機能と TFFR の定義及び Basic SIL であろうと思われる。この規格でこれまで最も注目されてきた SIL Table の変更のため、そう感じられると考えている。

一見すると、THR による SIL の定義が TFFR に置き換わっており、SIL table の定義が変わったように見える。

表 1　SIL Table (上 Edition 1.0 下 Edition 2.0)

Table A.1 – SIL-table

Tolerable hazard rate THR per hour and per function	Safety integrity level
$10^{-9} \le THR < 10^{-8}$	4
$10^{-8} \le THR < 10^{-7}$	3
$10^{-7} \le THR < 10^{-6}$	2
$10^{-6} \le THR < 10^{-5}$	1

Table A.1 – The SIL table

TFFR per hour and per function	Safety integrity level
$10^{-9} \le TFFR < 10^{-8}$	4
$10^{-8} \le TFFR < 10^{-7}$	3
$10^{-7} \le TFFR < 10^{-6}$	2
$10^{-6} \le TFFR < 10^{-5}$	1

Edition 1.0 の A.5.2 章には、“The SIL table identifies the required SIL for the safety-related function from the THR.”と記述されている。これによると、THR と整合する安全関連機能の tolerable rate である TFFR について、SIL を割り当てるということになり、Edition 2.0 は、TFFR という略語を定義したが、これは規格制定者が、TFFR は開発初期段階では考えづらい一方で、他の機能安全規格と整合させる目的で取り入れたことがコメントされており、誤解を避けるためであり、実質的に同じことを述べていることになる。一方、Basic SIL については従来の SIL 1 と SIL 0 の間に追加された区分である。

４．終わりに

本稿では、IEC 62425 の概要及び Edition 2.0 において変更された事項について概略を述べた。大きな思想として変更されてはいないが、全般として、取り扱いがあいまいな点が解消され、使い勝手がよくなっていると考えている。弊室としても、この規格をさらに解析し、よりよい認証体制を構築していきたいと考えている。関係各位のご指導をお願いしたい。

参考文献

1) IEC 62425 Editon 2.0, Railway applications – Communication, signalling and processing systems - Safety related electronic systems for signalling, IEC (2025-05)
2) IEC 62425 Editon 1.0, Railway applications – Communication, signalling and processing systems - Safety related electronic systems for signalling, IEC (2007-09)
3) IEC 60050 International Electrotechnical Vocabulary