国際規格における「機能安全」の重要性

鉄道国際規格センター　特任参与　川野 卓

1. はじめに

前回のコラムでは，鉄道システムの技術変化に伴い，全体を俯瞰して考える「システム思考」が重要であることをお伝えしました。これまでは「どのような技術を使うか」といった「手段」に重点を置いた安全マネジメントが行われてきましたが，システムが複雑化する現代では，「想定されるリスクとその対処方針」という「目的」に基づいた安全管理への移行が求められています。今回は，その中心的な考え方である「機能安全」について詳しく見ていきましょう。

2. 「本質安全」と「機能安全」の違い

安全を実現するアプローチには，大きく分けて「本質安全」と「機能安全」の2つがあります。鉄道と道路の交差部を例に挙げると，その違いが明確になります。

- 本質安全：鉄道と道路を立体交差にすることで，衝突事故のリスクそのものを物理的に排除する手法です。
- 機能安全：踏切を設けることで，衝突のリスクを許容できるレベルまで低下させる手法です。

理想的にはすべての場所を立体交差（本質安全）にすることが望ましいですが，費用や工期の面で現実的ではありません。そのため，適正なコストで高い安全性を実現できる「機能安全」の考え方を積極的に取り入れることが重要です。

3. 機能安全とフェールセーフ

「機能安全」とは，システムに安全を確保するための「機能」を組み込んでおくことで，リスクを許容できる範囲内に抑える手法のことです。

機能安全では，まず発生しうる「ハザード（危害の要因）」を想定リスクとして列挙します。その上で，「被害の大きさ」と「発生する頻度」により影響解析を行い，対策を講じることで，想定リスクをあらかじめ定めた「許容レベル」まで下げていきます。図3は機能安全の概念を図示したものですが，左側のギザギザで囲まれた「想定リスク」が影響解析・対策の結果，右側の円（許容レベル）の中に納まっており，これらのプロセス全体が機能安全の概念となります。

機能安全という言葉には，大きく分けて二つの捉え方があります。前述した踏切制御装置のように，安全機能を備えたシステム自体を指すこともありますが，



図1　本質安全のイメージ（立体交差）[1)]

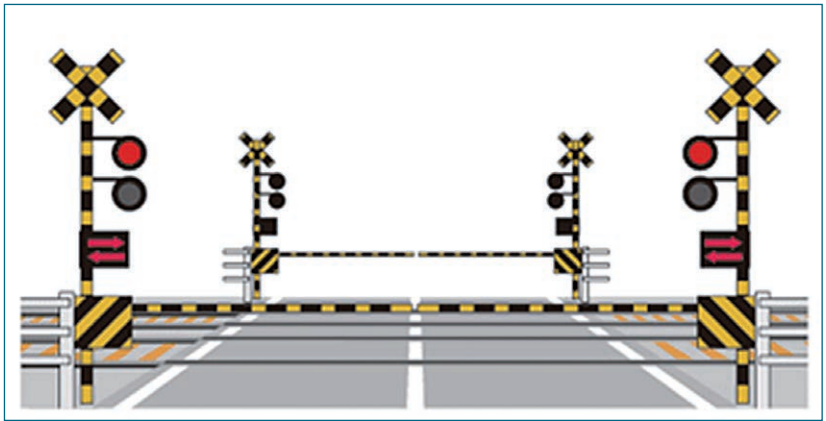


図2　機能安全のイメージ（踏切）[1)]

図3のように，プロセスも含んだ概念を含めて機能安全と言うこともあります。そのため，どちらの概念を指すかは前後の文脈で判断する必要があります。

踏切制御装置などの鉄道システムにおいて，機能安全を実現するための代表的な手法が「フェールセーフ」です。鉄道におけるフェールセーフとは，システムが故障した際に「衝突や脱線」といった危険な状態ではなく，「列車の停止」のような安全な状態に遷移させる確率を高める設計を意味します。

具体的には機能安全のプロセスに従い，想定リスクの影響解析を行い，可能な限りの技術的対策を施した上で，危険な故障の発生頻度を10万年に1回（10^{-9}/h）程度の許容レベルにまで落とし込む必要があります。なおこの許容レベルについては，さまざまな産業界において共通的に用いられており，社会的に受容される水準と考えることができます。

4. 鉄道分野の国際規格と機能安全の関係

機能安全の考え方は，電子化・ソフトウェア制御への依存が進み，複雑化したシステムにおいて安全性を確保する上で不可欠なものと言えます。機能安全は，IEC（国際電気標準会議）において「IEC 61508　機能安全規格」として2000年に制定されました。この規格は「電気／電子／プログラマブル電子（E/E/PE：Electrical/Electronic/Programmable Electronic）」を用いたシステムにおいて，故障・障害によって人命，環境，財産に影響を与えない方法論として世界中のさまざまな産業分野で活用されています。なお，産業分野ごとの機能安全規格も存在し，前回のコラムでも触れた「RAMS規格（IEC 62278）」も，鉄道分野に特化した機能安全のプロセスを定めた規格として2002年に制定されたものです。いずれの規格も，図3の概念を具体化するための手順や文書として記録すべき事柄が記載されており，少々理解しにくいのが難点です。

電子化・ソフトウェア制御への依存度の増大は，バグや仕様誤り，周囲環境からの電磁的な影響等による不具合のリスク増大につながります。また，サブシステムを多く含む複合化したシステムにおいては，サブシステム間の相互作用に起因する不具合が数多く発生しています。このような現状において，技術の実現手段にフォーカスした安全マネジメントには限界があります。そのため技術者個人の技量のみに依存することなく，想定リスクなどシステムの目的に立ち返り，定型化したプロセスや記録した文書に基づいて鉄道の安全性を作り込むRAMS規格，ひいては機能安全の意義を正しく理解し，活用してゆくことが重要であると考えます。

文　献

1）“いまさら聞けない 機能安全入門”，2009.6，MONOist，https://monoist.itmedia.co.jp/mn/articles/0906/15/news091.html（入手日：2026年8月1日）

2）“欧州の鉄道技術・日本の鉄道技術−RAMSと 海外と日本の鉄道の違いの紹介−”，2021.2，吉永 純，https://www.asahi-net.or.jp/~ZZ5J-YSNG/3-RAMS_FS/rams_1.htm（入手日：2026年8月1日）

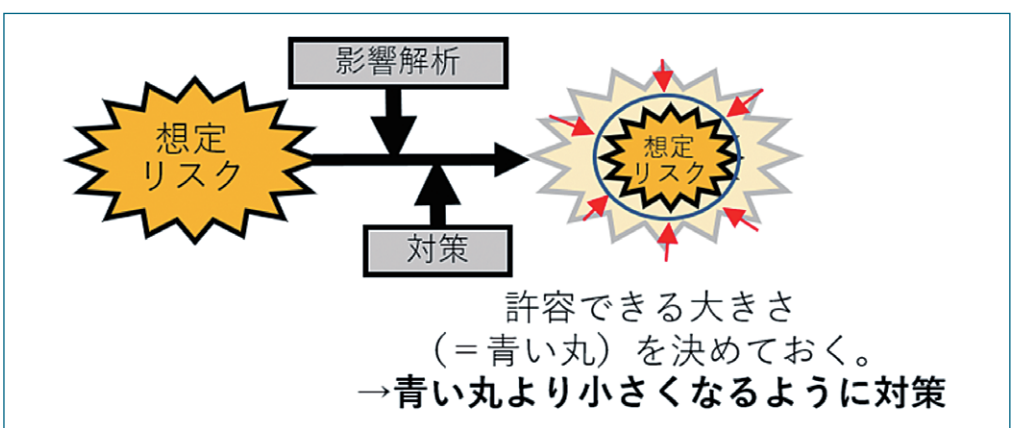


図3　機能安全の概念[2)]