

鉄道システムの第三者安全性評価と国際規格IEC 62425の接点について



交通システム研究部

※林田 守正

工藤 希

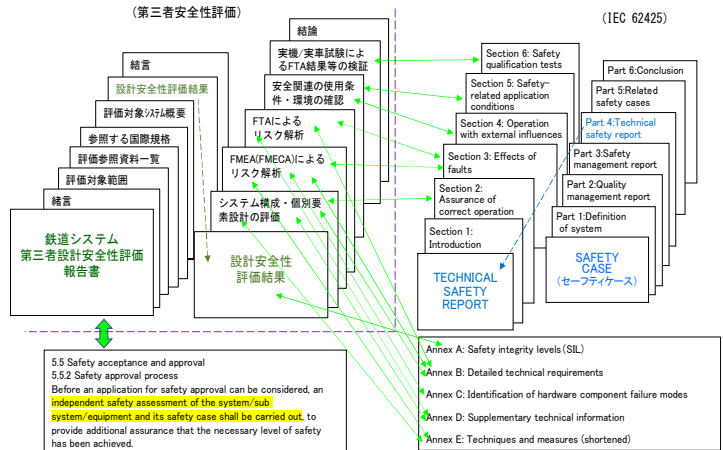
森 崇(鉄道認証室)

○概要

- ・当研究所では、長年にわたり、各種の鉄道に関する第三者安全性評価を行ってきた。
- ・近年、日本の鉄道システムの輸出に際しては、IEC (International Electrotechnical Commission) シリーズ等の国際規格への適合が求められる。
- ・主に信号システムのハードウェアに関する設計安全性評価と、それに関連が深いIEC 62425との接点に着目し、FTA (Fault Tree Analysis) 等のリスク解析を例として、フェールセーフ性の考え方やその担保の技法について考察した。

○安全性評価とIEC 62425の項目

- ・安全性評価結果の各項目と主に関連するのは、Safety Case Part 4: Technical Safety Reportの各Section。
- ・IEC 62425 Annex A～EにはSIL (Safety Integrity Level) の考え方、安全性を担保するための技術と対策等が記述されているため、安全性評価結果の各項目と対応。
- ・IEC 62425 5.5 Safety acceptance and approvalでは、システムの安全性の承認に際して、第三者安全性評価が必要。
- ・当研究所の安全性評価ではFMEA (FMECA及びFMEDAを含む) 及びFTAによるリスク解析を中核としているため、それらと関連が深いTechnical Safety Reportの下記との対応について考察。
- Section 2: Assurance of correct operation
- Section 3: Effects of faults
- Annex B及びAnnex E



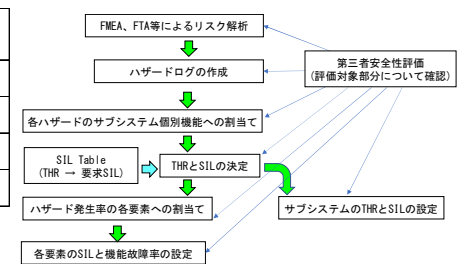
安全性評価報告書の項目例とIEC 62425の構成

○IEC 62425の安全性確保の考え方

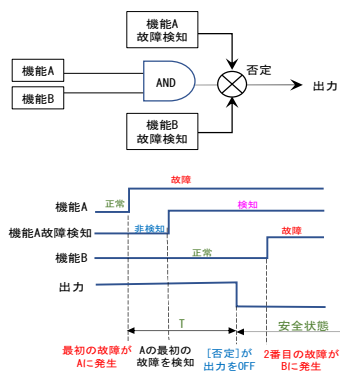
- ・対象システムに対してリスク解析を行いハザードログを作成
- ・認識された各ハザードのサブシステムの個別機能への割当てを行うことによってシステム機能としてのTHRを決定。
- ・THR (Tolerable Hazard Rate (/h))に応じて要求される機能毎のSILを、SIL Tableに沿って決定。
- ・これにより、サブシステムのTHRとSILが設定されると共に、ハザード発生率が各要素に割り当てられ、各要素のSILと機能故障率(/h)を設定。

許容可能なハザード発生頻度 (THR: 1時間/1機能当たり)	要求されるSIL (Safety Integrity Level)
$10^{-8} \leq \text{THR} < 10^{-7}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

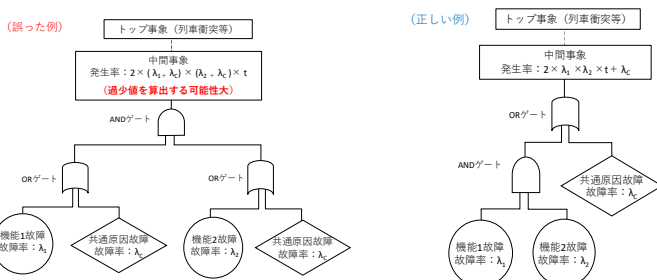
THRに応じたSILの割り当て



○OFTA・FMEAに関する検討



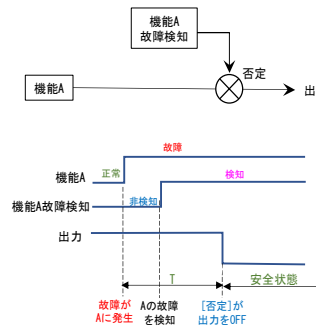
Composite fail safetyに相当するFTモデル



共通原因故障を含むFTA

○まとめ

- ・第三者安全性評価(自由形式)の国際規格IEC 62425との接点について考察し、国際規格の考え方を採り入れ、整合を図るに当たっての留意点を整理。
- ・今後、安全性評価とIEC 62425の他の項目、さらにIEC 62425以外の国際規格との接点について考察し、国際規格との整合性について引き続き検討。



Reactive fail safetyに相当するFTモデル

FMEAとIEC 62425 Annex E Technique & Measuresの対応

FMEAの例

要素	機能	故障モード	故障原因	故障の影響	対策	重大さ	発生頻度	リスク評価
a	地上電源	地上電力供給断	停電	地上信号保安システム機能停止	無停電電源装置	2	3	6
b	在線/非在線認識	非在線を在線と誤認	車両位置の誤認	当該軌道進入不能→列車遅延	位置検知精度向上	1	2	2
c	ATP信号送受信	在線を非在線と誤認	車両位置の誤認	他列車と衝突	高信頼装置の採用	4	1	4
d	ATP信号送受信	伝送中のデータ欠け	ノイズ	非常制動、出発不能→列車遅延	通信系統の二重化	2	2	4
e	ATP信号送受信	伝送中のデータ欠け	ノイズ	パターン生成条件錯誤→列車衝突	所定SMBの確保CRC検定等	4	1	4

IEC 62425 Annex E Technical Measures の例 (Table E.5 - Design features 抜粋)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Protection against operating errors	R: plausibility checks on each input command		HR: plausibility checks on each input command	
2 Protection against sabotage			R: additional organisational measures are necessary	
3 Protection against single fault for discrete components	R: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties		HR: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties	