カラーFTAによる信号システムの安全性評価

○［電］孫 佳 ［電］山本 正宣 ［電］望月 寛 ［電］高橋 聖 ［電］中村 英夫（日本大学）

Safety Estimation of Railway Signaling System using Color-FTA

○Ka Son, Masanori Yamamoto, Hiroshi Mochizuki, Sei Takahashi, Hideo Nakamura,
(NIHON Univ.)

A new safety analysis and estimation tool named a Color FTA is proposed. In a color FTA any basic event such as human error, software bug etc. is described by each different color symbol. The event occurrence phase of each element is aligned on a mission achievement cycle. Moreover, according to the occurrence probability of each event, the symbol size of each event is applied alternatively and visibility of FTA diagram is improved. The case study is also performed in this paper.

キーワード：安全性解析，FTA，カラーFTA，鉄道信号，使命達成サイクル
Key Words : Safety analysis, FTA, Color-FTA, Railway signaling, Mission achievement cycle

1．はじめに

RISK 管理棟で用いられる安全性解析手法の一つであるFTA（Fault Tree Analysis）は，トップイベントにおいたシステムの不具合事象の要因を詳細化していくアプローチである．このため，FTAはトップダウン的プローチといわれるが，解析の詳細さのレベルや網羅性は解析者のスキルに負うところが大きい．また，全体がツリー構造をしたグラフとして表現されるため，もう一つの安全性解析手法であるFMEA（Failure Mode and Effect Analysis）に比べ全体を把握しやすいといわれる．いずれにしても，FTAやFMEAを安全性解析ツールとして利用する場合には，網羅性と厳格性が必要であり，全ての事故事象に対する影響を評価しているか，また，評価は適切であるかの吟味が求められる．この点で，FTAやFMEAは静的な解析であり，システムの動作フェーズの影響に対する視認性が良くない．さらに，これらの解析は作業量が膨大になり，解析結果から，例えばソフトウェアに起因した障害の様相や,ヒューマンエラーに起因した障害の様相などを全体から抽出して評価することは容易でない．

このような現状に鑑み，筆者らは誤り要因を色別に表現するカラーFTAを提案した(1)．カラーFTAでは，例えば人間の扱いミスなどに特定の色を割り当てることにより，ヒューマンエラーのおおよその割合や，それがクリティカルな障害に結びつきかねないシステムであるか否かといった事柄が一目で分る．また，ソフトウェアに起因するものを色別にすることにより，全体の中でのソフトウェアバグの関わりが明瞭になる．

カラーFTAでは，縦軸に運用モードを取っており，システム挙動を考慮した安全性評価が可能となる．さらに，カラーFTAでは，要因の生起確率のオーダを記号○の大きさで表現する．このことにより，個々の数値を確認しなくても，要因の発生確率の概要が把握できる．

本報告では，カラーFTAの記述方法を紹介し，電子閉塞システムに適用した場合のケーススタディ結果を示す．

2．カラーFTAの記述方法

2.1 使命達成サイクルによる類別

カラーFTAは，縦軸に使命達成サイクルの各フェーズをとり，FTAにおける障害や故障原因は，それが作用するフェーズの領域上に配置する．各フェーズにはシステムの使命達成サイクル中における占有割合が出され，領域の故障フェーズは，占有割合を乗じた分だけシステムにとって影響することになる．

2.2 要因カテゴリによる類別

本文事故は装置の故障以外に人間の取扱いミスに起因するものや，装置故障にもハードウェアの故障によるものとソフトウェアの誤りに起因するものがある．従来のFTAでは，これらが，同一のレベルで記述されていたため，ヒューマンに起因するもの，ハードウェアに起因するもの，ソフトウェアに起因するものの関係が判断できなかった．カラーFTAは，それぞれ異なる色を用いて識別できるよう

にする．

2.3 生起確率の表現

通常の FTA の場合，基本事象の発生確率はシンボルに添えて表記されるが，カラーFTA では，確率値のオーダに基づいてノードの大きさにも割当てられ表現される．このため，各基本事象のカテゴリの分布の様子が視覚的に把握できると共に解析の見通しが良くなる．

3．ケーススタディ

カラーFTA のケーススタデイとして，地方交通線で稼働している「電子閉塞システム」を対象に解析を実施した．解析のレベルは，サブシステムの障害程度とした．解析において用いた故障率は，時間当たりであり，1 年間に 1 回の確率で発生するものは，1.1×10^{-4}(1.1E−4 と表記)になる．なお，値はカラーFTA を説明するために仮定した，主観的値であり，フィールドのデータではない．

図中左列は使命達成サイクルのフェーズであり，数値は，その中の割合を示す．使命達成サイクル時間が T 時間であると，解析で得られたトップイベントの生起確率に T を乗じた値が，実際の確率ということになる．この解析に従えば，T が増加すれば生起確率も大きくなり，「事故の発生頻度が，列車本数や走行キロに応じて変化するという」傾向を表現できることを意味する．このことも従来の静的な FTA では得られないカラーFTA の効果といえる．

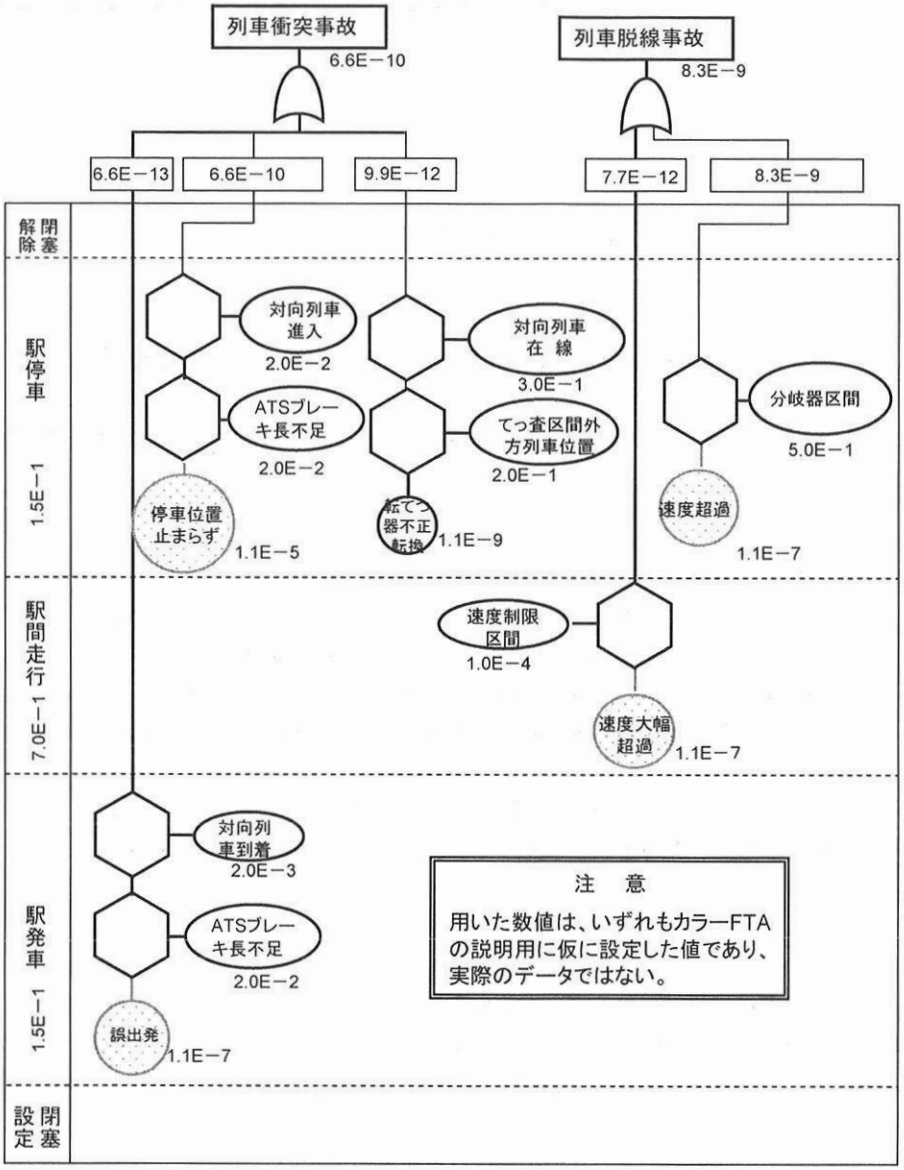

図 1．電子閉そくを例にしたカラーFTA による解析

値は主観的とはいえ，解析結果によると，次のような事柄が得られた．

①列車衝突事故は，列車脱線事故よりも頻度は小さい

②列車衝突は，駅停止時の誤りに起因するものが大きく，誤出発は，誤出発の頻度は多いもののそれがそのまま衝突事故に結びつくものではない

なお，解析においてヒューマンエラーに依るのか機器故障に依るのかといった判別も瞬時にでき，カラーFTA の効果が確認できた．なお，図 1 では，ヒューマンに起因したノードを赤色の網掛けで記している．

4．あとがき

FTA を発展させた，カラーFTA を提案し，地方交通線に導入されている「電子閉塞システム」に適用して効果を確認した．

FTA の限界と言われた，システムの使命達成サイクを通した評価が可能となるほか，基本事象にカラーを割当てることによる識別性の向上など，意図した効果が確認できた．使命達成サイクルを考慮しない従来の FTA と比べると，全体としては粗な解析図となるものの見通しの得やすい解析図となった．

今回は，事象の生起確率等については，主観的な値を与えたが，実用時にはいかにしてデータを得るかが鍵となる．今後，データを与えれば，基本事象や制約条件の記号の大きさが自動的に与えられるようなツールに展開したいと考えている．

参　考　文　献

1) 孫佳，望月寛，高橋聖，中村英夫，山本正宣：カラーFTA による信号システムの安全性評価，電学研資 TER10-032，2010.