平成29年度 情報工学コース卒業研究報告要旨

高田・本田 研究室	氏　　名	戸 田　佳 成
卒業研究題目	機能共鳴モデルに対するハザード分析手法 FRAM/STPA	

本研究では，Safety-II と呼ばれる新しい安全に対する考えからスタートした．Safety-II は，Erik Hollnagel 氏によって提案された考えであり，従来の安全の定義「不具合のない状態」という安全に対する考えを Safety-I と呼び，Safety-II を「許容可能な状態が維持されている状態」と定義する．また、Erik Hollnagel 氏は，Safety-II のためのモデリング言語，機能共鳴分析手法 FRAM(Functional Resonance Analysis Method) を提唱している．

FRAM はモデリング言語であり，システムの機能を定義し，機能間の関係を示すことでシステムを表現する．一つの機能は六角形で表現され，6 つの側面から定義される．側面は，入力，出力，時間，事前条件，制御，資源で構成される．機能の出力は他の機能に一致する側面がある場合にはその要素間が線で結ばれ，機能間の関係が表現される．FRAM の使用例は少なく，具体例も少ないという課題がある．そのためモデルの記述方法に明確になっていない部分が多く存在する．さらに，具体的な安全分析方法に関しては提唱者である Erik Hollnagel 氏も検討段階であり，まだ明確になっていない．

本研究では，FRAM を用いたモデル例を作成し，記述方法を理解する．次に，FRAM に対する安全分析手法として FRAM/STPA を提案する．検出されたハザードによる比較、評価を実施し，FRAM/STPA の網羅性を明らかにすることを目的とした．モデルの記述方法は，モデリングするシステムを抽象度の高いモデルから記述し，次第に抽象度の低いモデルの記述へと移行する方針をとった．理由は，FRAM ではシステムの機能の 6 つの側面を正確に書くことが重要になるため，トップダウンに書くことにより記述漏れを削減するためである．また，暗黙的な条件について記述することも FRAM の特徴の一つであり，システム設計者や利用者が見逃しがちな暗黙知を含めた分析が可能になる．これらに注意しモデル記述を行った結果，いくつかの FRAM の具体例が作成でき，記述手順についても検討が行えた．

安全分析の方法は，STPA(STAMP based Process Analysis) によるハザード分析手法を FRAM に適用した．分析対象は踏切システムを採用した。踏切は、列車の接近を検知すると警報機の鳴動と遮断機の降下を行う．警報機、遮断機の降下の後には、列車の通過中に対向列車が接近した際に重複して警報機、遮断機が機能しないようにマスクを行う．列車の通過を検知すると，マスクを解除し、警報機の停止、遮断機の上昇を行う．最初に FRAM で踏切システムをモデリングを行ない、作成したモデルに対してハザード分析を行なった． STPA のガイドワードを，FRAM に置ける各機能の 6 つの側面それぞれに対して当てはめ，ハザードを検出した．その後同じシステムに対して STAMP(Systems-Theoretic Accident Model and Process)/STPA を行い、検出された結果と FRAM/STPA によって検出された結果を比較した．

比較の結果，FRAM/STPA では STAMP/STPA で検出したハザードのほとんどを検出することが出来た．しかし，STAMP/STPA で検出されたハザードの内，具体的なシステムの構成要素に関するハザードを見落としてしまった．一方，FRAM/STPA では STAMP/STPA に比べ多くのハザードの検出を行えた．具体的には，資源や前提条件に関する暗黙的な要素に対するハザードの検出，同様のハザードの発見に対しても FRAM/STPA ではハザードを数種類の原因に分類して検出することが可能であった．これらにより，FRAM/STPA を使用することで，対象におけるハザードをより網羅的に検出することが可能であることが確認できた．