PS-1　自動運航船のリスク解析手法の構築に向けた試み

海洋リスク評価系　＊塩苅　恵，伊藤　博子，柚井　智洋

1. はじめに

近年，自動運航船の開発プロジェクトが数多く立ち上げられ，関連する様々な技術開発が行われている．自動運航船の試験運航や実用化にあたっては，新技術を特定の条件下で運用した場合の安全性を確認する手法が重要な役割を果たすと考えられ，そのためのリスク解析手法が必要となる．

従来のリスク解析手法は主にハードウェアを対象に開発されており，自動運航船のようにソフトウェアを多く含む複雑なシステムにはそのままでは適用しにくい．当所では，自動化システムが重要な役割を担う運航形態とそれを支える自動化システムのためのリスク解析手法の確立をめざし，従来のリスク解析手法と，ソフトウェアを含むシステムを対象とした新たな解析手法及び，ソフトウェアシステムの設計技術等を調査し，それらの特徴や解析結果等を比較し，その結果に基づき新しい手法を開発しているので紹介する．

2. 新規手法の調査と従来手法との比較

自動運航船のような複雑なシステムのリスク解析手法として，STAMP (Systems-Theoretic Accident Model and Processes)/STPA (System-Theoretic Process Analysis)[1]が注目されている．これは，拡張した事故の因果関係モデルに基づいた，比較的新しいハザード解析手法であり，システムの構成要素を抽象化して，要素間の相互作用に着目することで網羅的にハザードの解析を行うことができる．

山口ら[2]は要件定義工程でSTAMP/STPAを，詳細設計工程以降でFMEA (Faulure Mode and Effects Analysis)[3]を実施することで，互いに競合せず，より包括的にシステムの安全解析ができると述べている．Sultana et al.[4]は高度な自動化システムを含み要素間の相互作用が多い複雑なシステムにはSTAMP/STPAが，相互作用が単純でソフトウェアが少ないプロセスシステムにはHAZOP (Hazard and Operability Studies)[3]が適している可能性があると述べている．

自動運航船のリスク解析においては，ハードウェア，ソフトウェア及び人間の間の相互作用に潜むハザードの解析も重要になると思われ，システム全体を網羅的に捉えることが可能なSTAMP/STPAのような手法が適していると考えられる．また，山口ら[2]の主張のように，設計段階によって解析手法を変える方法や，自動運航船のシステム全体を対象にSTAMP/STPAで解析し，特に詳細に解析したいサブシステムについては部分的にHAZOPやFMEA等の手法を用いて詳細解析を行う方法も考えられる．

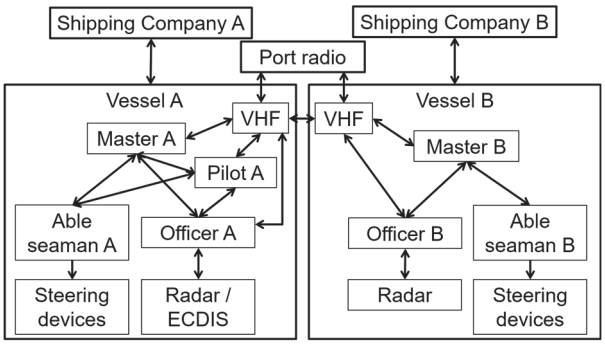
3. STAMP/CASTによる船舶衝突事故原因分析

自動運航船のシステム全体に対してSTAMP/STPAによるリスク解析を行うことに先立ち，同手法と基本概念を共有し，解析上の共通点の多いSTAMP/Causal Analysis using System Theory (CAST)[1]を船舶衝突事故に適用して事故原因の分析を行うことで，STAMP/STPAによる解析に必要な知見を得た[5]ので紹介する．

3.1　分析対象と分析手法

神戸中央航路で平成28年6月7日に発生した2隻のコンテナ船（A船及びB船とする）による衝突事故[6]を対象に，STAMP/CASTの手法を利用して事故原因を分析した．

運輸安全委員会の報告書[6]中では，人間の認知的側面に着目した人間信頼解析手法の一つ，CREAM（Cognitive Reliability and Error Analysis Method）を利用した分析がされている．一方，今回利用したSTAMP/CASTでは，認知過程の解析まではガイドされていない．そこで，今回はSTAMP/CASTに，人間の意思決定過程のモデル化手法であるNDM (Naturalistic Decision Making) モデルを導入することで対応した．CREAMもNDMモデルも人的要因を陽に考慮した手法であるが，STAMPのように人間と機械の関係を陽に定義する枠組みは提供されていないため，STAMP/CASTによって人間と機械を含むシステム全体の制御構造をモデル化し（図－1），その制御の問題として対象システムにおける安全上の問題点を分析した．



図－1　A船とB船の衝突事故原因分析のための安全制御構造図[5]

3.2　分析結果を踏まえた分析手法に関する考察

分析の結果は，公式の報告書による分析結果[6]と概ね一致し，妥当性が確認できた．STAMP/STPAにも，今回のSTAMP/CASTによる解析と同様に，CREAMの認知過程の分析手順やNDMモデルを導入することで，人間の認知過程の解析をガイドすることが可能になると考えられる．

4. ソフトウェアを含むシステムのリスク解析

自動運航船のシステムを対象としたリスク解析手法の開

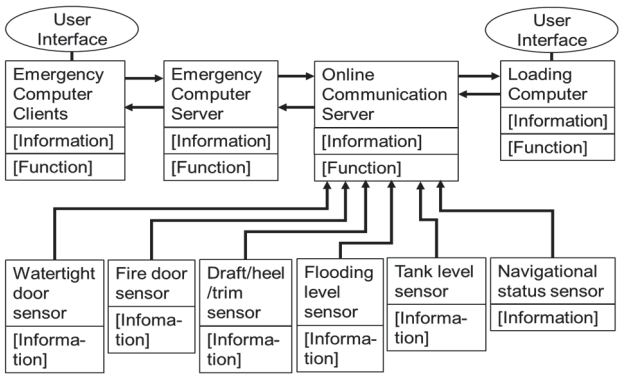
発を見据えて，ソフトウェアを含むシステムを対象にリスク解析を行う手法を開発した[7]ので紹介する．

4.1 解析対象と解析方法

ソフトウェアを含むシステムの一例として，NAPA 社製の Emergency Computer (EC)[8]を対象に，SWIFT (Structured What IF Technique)[3]による解析を行った．

SWIFT ではワークシートを利用して，専門家チームによるブレインストーミングで通常操作からの逸脱を抽出する．解析対象を事前に定義することで対象物や使用する局面を明確化し，解析作業を促進するが，今回は解析対象にソフトウェアを含むため，システムの各構成要素が所持する情報群と各構成要素が行う操作，構成要素間の相互作用を明に定義する必要があった．

そこで，ソフトウェアのモデリング手法を標準化した UML (Unified Modeling Language)のダイアグラムのうち，静的モデルの一つであるクラス図[9]を応用し，ソフトウェアとハードウェアの両方を含むシステムのモデル化を行い（図－2），構成要素ごとにワークシートを作成してハザードを同定した．また，各ハザードの発生頻度と結果の重大性を，FSA ガイドライン[10]に従って決定し，リスク指数（Risk Index: RI）を算出することで，半定量的に各ハザードのリスクの大きさを評価した[10]．



図－2 UML のクラス図を応用して作成した EC システムのモデル図[7]（各構成要素が有する情報群と操作のリスト及び構成要素間の相互作用（入出力）の記載は省略）

4.2 解析結果を踏まえた解析手法に関する考察

解析の結果，全部で 130 のハザードとそれらの RI の値が同定された．これらのハザードに対し，RI の値が大きいものから優先的に追加の防御策を提案した．

開発した手法により，ソフトウェアを含むシステムのモデル化と SWIFT による解析が可能になった．SWIFT は設計初期段階から詳細設計段階まで幅広く適用でき，これから開発される自動運航船の新たなシステムにも適用できる可能性が高い．ただし，システムのモデル化において，本研究ではソフトウェア内部機能の記述が必要であることを考慮して UML を応用したが，設計初期段階でソフトウェア内部まで定義する必要のない場合は，STAMP によるモデル化が適している可能性もあり，その場合，STAMP でモデル化したシステムを SWIFT で解析するという組み合わせも考え得る．また，効率的なハザード同定のために STAMP/STPA で使用されるガイドワードの SWIFT への応用も考えられ，これら手法の適性や組み合わせの可能性については更なる検討が必要である．

5. まとめ

文献調査によって，自動運航船のリスク解析手法に必要な要素を明らかにし，新規手法として STAMP/STPA が有用であることが分かった．合わせて，設計段階に応じて最適な手法を選択することや，部分的に従来手法を用いて詳細解析を行うことも有効である可能性を明らかにした．また，NDM モデルを導入した STAMP/CAST による船舶衝突事故の原因分析や，UML を応用してソフトウェアを含むシステムをモデル化し，SWIFT で解析する手法の開発とその有用性の確認を行った．

今後は，STAMP と UML の両モデル化手法と，STPA と SWIFT の両解析手法の長所を活かした新規手法の検討や，新旧手法の組み合わせやそれらの接続についても検討が必要となる．

謝辞

本研究で実施した NAPA 社製の Emergency Computer のリスク解析は，日本海事協会及び NAPA 社の協力を得て実施したものです．関係各位に深く感謝申し上げます．

参考文献

1) Leveson, N. G.: Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press (2012).
2) 山口晋一ほか：STAMP/STPA によるハザード影響度に基づく逐次的な安全解析方法の構築評価，安全工学学会誌，58 巻 2 号 (2019)，pp.124-132.
3) 三友信夫：リスク評価について，海上技術安全研究所報告，8 巻 4 号特集号 (2008)，pp.1-9.
4) Sultana, S. et al.: Hazard analysis: Application of STPA to ship-to-ship transfer of LNG, J. of Loss Prevention in the Process Industries 60 (2019), pp.241-252.
5) 柚井智洋ほか：船舶事故の要因分析への STAMP/CAST の適用－自動運航船の安全性分析に向けて－，日本船舶海洋工学会講演会論文集 30 号 (2020)，pp.165-168.
6) 運輸安全委員会：船舶事故調査報告書，MA2018-2 (2018).
7) 塩苅恵ほか：自動運航船のリスク解析手法の構築に向けて，日本船舶海洋工学会講演会論文集 30 号 (2020)，pp.393-396.
8) Pennanen, P. et al.: Integrated decision support system for increased passenger ship safety, Damaged ship III, The Royal Institution of Naval Architects (2015).
9) 井上樹：ダイアグラム別 UML 徹底活用 第 2 版，翔泳社 (2018).
10) IMO document: MSC-MEPC.2/Circ.12/Rev.2, Revised guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process (2018).