様式 C-19

科学研究費補助金研究成果報告書

平成　21　年　5　月　27　日現在

研究種目：基盤研究(C)
研究期間：2007～2008
課題番号：19510170
研究課題名（和文）　動的な機能関係を持つ複雑なシステムの故障分析

研究課題名（英文）　Failure Analysis of Complex Systems with Dynamic Functional Relations

研究代表者
幸田　武久　(TAKEHISA KOHDA)
京都大学・大学院工学研究科・准教授
研究者番号：　60205333

研究成果の概要：
　システムの機能構造が時間ともに変化する複雑なシステム、フェーズドミッションシステム（PMS）では、その各作業段階での故障発生原因は目的機能とともに変化し、また故障確率も断続的に変化する。また故障が発生した時にはその原因候補を推定するのに故障発生前のフェーズとの機能関係を考慮して、潜在的故障原因を検討する必要がある。本研究では、このような特徴を有する PMS の故障分析方法の確立を試みる。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,600,000	480,000	2,080,000
2008 年度	1,200,000	360,000	1,560,000
年度			
年度			
年度			
総　計	2,800,000	840,000	3,640,000

研究分野：複合新領域
科研費の分科・細目：社会・安全システム科学　社会システム工学・安全システム
キーワード：安全工学、故障分析

１．研究開始当初の背景
(1)　従来のシステム故障分析では、重大な損害を引き起こし得る潜在的機能障害の同定に焦点があてられていたが、一般的なシステムでは各運用段階で種々の機能が組み合わされ、各運用段階において要求される機能も異なり、システム機能達成はこれらの異なる機能の組み合わせとして実現する必要がある。しかし、このような異なる機能の分析を行う適切な解析方法はなかった。
(2)　システム構造が時々刻々と変化するので、ミッションを通しての平均的な機能信頼度より、ミッションを通して故障発生確率が最大となる時点やリスクが最大となる時点の同定が問題となり、このためにはミッションを通した故障確率の時間的変動を分析する必要がある。
(3)　システムの要求機能がフェーズごとに変化するフェーズドミッションシステム(PMS)で。各フェーズで要求される機能に関連した故障モードを考慮した、系統的なリスク分析方法は確立されていなかった。むしろ、PMS 研究では、当初からミッション信頼度の評価に重点が置かれていた。
２．研究の目的
(1)　本研究の目的は、システム運用段階で要

求機能に応じてシステム機能構成が変化する PMS を対象として、そのミッションを通じて事故発生確率を評価し、システム故障発生に寄与する因子を抽出し、設計の改善を図り、リスク低減方法の確立を目的とする。

(2) PMS の特徴である、フェーズの切り替え時に発生する事故発生確率の急激な変化、すなわち、その前のフェーズでは現れなかった潜在的故障の顕在化の低減策について考える。特に要求機能が変わることにより故障確率が大幅に変動する場合には、運用点検や保守保全の手順が重要となる。

３．研究の方法

PMS はフェーズごとに異なる機能要求が順番に達成するシステムであり、各要素に要求される機能も段階に応じて異なる。従って。一つのシステム機能のみに着目してフェーズ毎に単独に解析すると、フェーズ切り替え時の急激な変化は説明できず、現時点までのフェーズの状態変化を考慮する必要がある。また、PMS の改良を検討するには、システム故障確率の定量的な解析のみでなく、システム故障原因を系統的に同定する定性的な解析が必要である。本研究では、まず PMS の各フェーズで故障する条件（最小カットセット）を求め、それに基づいてシステム故障確率の動的変化を求める。分析手順の概略は次のようになる。

(1) 各フェーズでの正常状態・故障状態の導出

一般的なシステムの信頼性・故障分析では、分析対象とするシステムレベルの故障状態を明確に定義して、そこから「どうしてそのような故障事象が生じたのか？」という問いかけを反復して分析しながら、システム故障と要素故障原因との因果関係を導出するトップダウンの解析方法である FTA(Fault Tree Analysis)が広く用いられている。本研究では、まず FTA で各フェーズでのシステム故障発生原因を導出する。手順は以下のとおりである。

① システム故障（頂上事象：システムにとって望ましくない事象）の定義

② システム故障発生論理の同定

要因間の論理関係を、基本的には AND（上位事象が発生するためにはすべての下位事象が発生しなければならない）と OR（下位事象のいずれかが発生すると上位事象が発生する）の論理関係で表現しながら、FT（Fault Tree）を展開する。

③ 定性的分析

②で得られた FT に基づいてシステム故障発生が起こり得る基本事象（要素故障）の最小組み合わせ（最小カットセット）の導出。

④ 定量的分析

システム故障はいずれかの最小カットセットが成立すれば発生するので、いずれかの最小カットセットが発生する確率としてシステム故障発生確率を得る。

⑤ システム故障に対する要素故障の感度解析を行って、システム故障発生の低減を図る。要素故障確率を用いて、事故発生確率を定量的に評価する。

FTA で得られる最小カットセットや最小パスセットは、それぞれシステムがある要求機能に対して、故障状態か、正常状態であるかを表現するのみで、事故連鎖や事象間の従属性は明確に表現できない。さらに、PMS での故障発生には、あるフェーズまでは正常であったが、次のフェーズで突然故障状態に至ったという事象系列が含まれる。システム故障直前の要求機能とシステム故障時点での要求機能が必ずしも一致せず、潜在化していた故障モードがフェーズの変化で顕在化するのである。

(2) PMS の故障発生条件

PMS の故障は、その時点での要求機能が満たされていないかどうかに依存して発生する。最小カットセットのいずれかの状態が存在するとそのフェーズでのシステム故障が発生する。逆に、最小パスセットの状態が存在すれば、システム故障は発生していない。従って、PMS では、事象の発生を考える場合は、「どの時点で、」「どの要素が、」「どのような状態（故障モード）に」あるかを明確にしなければならない。

システムあるいは要素の状態変化、いわゆる事象発生も、状態変化として表現できる。要素 i の故障モード j が時点 t1 から時点 t2 で発生する事象は、

{要素 i が時点 t1 で正常状態}
　∧{要素 i が時点 t2 で故障モード j}

と故障が発生する時点の開始点と終了点における要素状態で表現できる。ここで、∧は論理的 AND を表す。同様に時点 t1 から時点 t2 の間のシステム故障発生についても同様に、

{システムが時点 t1 で正常状態}
　∧{システムが時点 t2 で故障状態}

と表現できる。

PMS はフェーズが異なると要求機能が変わるのでフェーズ 1 からフェーズ i まで正常であることは、各フェーズの終了時刻でそのフェーズでの要求機能が満足する必要がある。そこで、

{PMS がフェーズ 1 から i まで正常}
={PMS がフェーズ 1 の終了時刻で正常}
∧・・・∧{PMS がフェーズ i の終了時刻で正常}

と表現される。

PMS がフェーズ i で故障するとは、PMS がフェーズ i-1 まで正常で、その後システム故障状態に至ることである、したがって、PMS がフェーズ i で故障する事象は、

{PMS がフェーズ i で故障する}
={PMS がフェーズ 1 の終了時点で正常}
∧・・・∧{PMS がフェーズ i-1 の終了時点で正常}∧{システムがフェーズ i の終了時点で故障}
と表現できる。

各フェーズでの故障状態は(1)の FTA で得られた最小カットセットの論理積の論理和で、正常状態は最小パスセットの論理積の論理和でそれぞれ表わされる。これらを PMS のフェーズ i での故障条件に代入して、論理展開を行い、簡単化すると、システム故障発生条件の最小カットセット表現（論理積の論理和）が得られる。

なお、議論を簡単にするため、以下では要素と PMS に対して次のような仮定をする。
A1) PMS が稼働開始時点では、システムも要素も新品同様で、正常状態である。
A2) システムも要素もミッション稼働中は、修理は施されない。故障はシステム故障が発生するまで放置される。
これらの仮定は、要素やシステムが稼働中に故障すると、システム故障が発生するまで稼働状態に復帰することはないことを意味する。

(3) PMS の故障発生確率

PMS の故障発生確率は、(2)で得られたフェーズ i での基本事象による故障発生条件に対する期待値操作を行って計算するか、確率計算における一般的方法である包除法（Inclusion & Exclusion Method）を用いて行う。

また、各時点における基本事象（要素故障）の発生確率は、各要素は故障メカニズムの異なる故障モードを持つ（競合リスクモデル：最初に発現した故障モードのみが発生する）を用いて計算する。最も単純なケースとして、各故障モードの故障発生率が一定で、ミッション開始時点で新品同様な状態であったとする。時点 t において要素 i が正常状態にある確率 $R_0(t)$、故障モード j の状態にある確率 $F_i(t)$は、それぞれ次のように得られる。

$$R_0(t) = \exp\{-\sum_{j\neq 0}\lambda_j t)$$

$$F_i(t) = \frac{\lambda_i}{\sum_{j\neq 0}\lambda_j}\left(1-\exp\{-\sum_{j\neq 0}\lambda_j t)\right)$$

例えば、フェーズ 1 で要素 1 が正常で、フェーズ 2 で要素 1 が故障モード 1 になるという事象 A は、
事象 A
={要素 1 はフェーズ 1 の終了時点で正常}
∧{要素 1 はフェーズ 2 の終了時点で故障モード 1}
と表され、その状態確率は

$$R_0(t_1^e)F_1(t_2^e) = \exp\{-\sum_{j\neq 0}\lambda_j t_1^e)$$
$$\times\frac{\lambda_1}{\sum_{j\neq 0}\lambda_j}\left(1-\exp\{-\sum_{j\neq 0}\lambda_j (t_2^e - t_1^e)\}\right)$$

となる。要素 1 はフェーズ 1 で正常であることはフェーズ 2 における前提条件になるので。要素 1 の故障モード 1 の遷移はフェーズ 2 の開始時点から始まる。この際、正常確率はフェーズ 1 の残存分となる（第一項）となる。このように、ある時点で要素が正常状態にあると判明すれば、その時点以降の故障モードに対する条件があれば、その事象の発生確率は正常と判明した時点からの経過時間にその故障モードに遷移した確率として計算される。

(4) 計算例

フェーズ 1 では並列システム（両方が故障すればシステムが故障）、フェーズ 2 では直列システム（いずれかが故障すればシステム故障）からなる 2 フェーズからなる PMS を考える。
① 各フェーズの最小カットセットは、
フェーズ 1 ：{(1,1,1),(2,1,1)}
フェーズ 2 ：{(1,2,1)},{(2,2,1)}
と得られる。同様に、最小パスセットは
フェーズ 1 ：{(1,1,1)},{(2,1,1)}
フェーズ 2 ：{(1,2,1),(2,2,1)}
となる、ここで、(i,j,k)は要素 i がフェーズ j で故障モード k にある（ない。最小パスセットの場合）ことを示す。
② PMS の故障発生条件
各フェーズで初めて故障する発生条件を求める。フェーズ 1 では、稼働開始後の故障発生で、発生条件
{(1,1,1),(2,1,1)}
は、並列システムの故障確率と同等である。

フェーズ 2 で初めて故障する場合は、フェーズ 1 の部分は並列システムの最小パスセットをとって正常状態であり、フェーズ 2 の部分は直列システムの最小カットセットで故障状態が表現される。したがって、
{フェーズ 2 でシステム故障発生}
={(1,1,-1)}∨{(2,1,-1)}∧{(1,2,1)}∨(2,2,1)}
=(1,1,-1) (1,2,1)∨(2,1,-1) (1,2,1
∨(1,1,-1) 1,2,1)∨(2,1,-1) (2,2,1)
=(1,1,0) (1,2,1)｜(1,1,0)∨(2,1,-1) (1,2,1)
∨(1,1,-1) 2,2,1)∨(2,1,0) (2,2,1)｜(2,1,0)
ここで、(i,j,k)は要素 i がフェーズ 2 で故障モード k にいることを、(i,j,k)｜(i'j',k')は後者の条件における前者の発生を、∨は論理的 OR をそれぞれ表す。
③ 故障発生条件の定量的評価

論理積に現れる要素名が異なる場合は、論理積表現に現れる要素は独立であり、確率計算では各要素モデルの積で計算できる。要素

名が同じで、前後する故障モードが異なる場合は、以下のように変形できる。
・前の条件表現が後に現れる故障モード表現の否定（故障モードが発生していない）であれば、後の故障モードを正常モードの条件付き発生確率（前のフェーズの終了時間に正常状態にある確率を初期状態の存在確率として計算した故障モードにある存在確率）とする。
・後がある故障モードの否定で、前が同じ故障モード状態にある場合は、その論理積は存在しない。

先ほどの例に適用すると、

Pr{フェーズ２でシステム故障発生}
=Pr{(1,1,0)}Pr{(1,2,1)｜(1,1,0)}
＋Pr{(2,1,-1) (1,2,1)}＋Pr{(1,1,-1) (2,2,1)}
＋Pr{(2,1,0)}Pr{ (2,2,1)｜(2,1,0)}

なお、ここでは計算を簡単にするため、稀有事象近似（各発生確率が小さいので高次の積は省略）を用いた。また、Pr(A)は事象 A の発生確率を、Pr{A|B}は事象 B が発生した下での事象 A の発生確率を表す。また、各基本事象の発生確率の計算は、3(3)にある確率の計算式に基づいて計算できる。

４．研究成果

本研究では、時間の経過化とともに機能論理が変化するフェーズドミッションシステム(PMS)の論理的アプローチによる新たな故障分析方法を開発した。その特徴として次のような点がある。

(1) 一般的なシステムは段階ごとに異なる機能を実行する PMS とみなすことができるので、一般的なシステムに適用可能な故障分析・リスク解析方法を開発した。

(2) 各段階での要素に対する機能要求が変化するので、各要素に対して複数の故障モードを考慮できるようにした。

(3) PMS の各フェーズでの動的な故障発生確率を導出することにより、クリティカルな部分を明瞭に示すことができるようにした。

(4) 「どの要素、いつ、どのような故障モード」にあるかという表現を用いることにより、得られたシステム故障の事故連鎖の意味が理解しやすいようにした。

開発した分析方法は、論理的アプローチであるので、大規模なシステムへの応用を考えると、論理計算は確率計算で変数の組み合わせ的爆発が考えられるので、モジュールのような独立して解析できる方法を検討したい。また、実際的な問題に適用して、手法の改善を行いたい。

動的に機能論理が変わる PMS に関しては、ミッション信頼性の評価が主体であったが、今後いくつかの動作モードを持つシステムをどのように運用するかの問題も、信頼性、保全性、稼働率の面等から検討したい。また、確率評価の基礎となる定性的論理モデルの構築には関する合理的なシステム故障論理モデルの作成を検討したい。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計 6 件）

① Takehisa Kohda, Accident Occurrence Evaluation of Phased-Mission Systems Composed of Components with Multiple Failure Modes, ESREL 2008 & 17th SRA Annual Conference, 2008.9.22, ﾊﾞﾚﾝｼｱ ﾎﾟﾘﾃｸﾆｶ大学、ｽﾍﾟｲﾝ
② Takehisa Kohda, Satoshi Matsumoto, Masaki Nakagawa, Risk Analysis of Phased-Mission Systems with Multiple Failure Modes, RAMS2008, 2008.1. 28-31, 2008, the Palace Station Hotel & Casino, Las Vegas,Nevada. USA
③ 幸田武久、フェーズドミッションアプローチによるバッチプロセスの定量的リスク評価、第 42 回化学工学コロキウム、2008 年 1 月 8 日、岡山大学
④ 松本智史、幸田武久、中川昌樹、フェーズドミッションアプローチによるバッチプロセスの定量的リスク評価、第 40 回安全工学研究発表会、2007 年 12 月 7 日、パシフィコ横浜
⑤ Takehisa Kohda, Satoshi Matsumoto, Masaki Nakagawa, Accident Analysis of Batch Processes using Phased Mission Systems Approach, Asia Pacific Symposium on Safety 2007, 2007.11.1, Westin Choun Hotel, Busan, Korea
⑥ 松本智史、幸田武久、中川昌樹、複数故障モードを考慮したフェーズドミッション分析、安全工学シンポジウム 2007、2007 年 7 月 6 日、日本学術会議

６．研究組織

(1)研究代表者

研究代表者
幸田　武久　(TAKEHISA KOHDA)
京都大学・大学院工学研究科・准教授
研究者番号：　60205333