システムの安全性・信頼性分析手法

SEC調査役　三原　幸博　SEC調査役　十山　圭介　SEC調査役　石井　正悟
SEC研究員　松田　充弘　SEC調査役　三縄　俊信　SEC主任　八嶋　俊介

システムの安全性・信頼性の分析をテーマとして、障害原因診断WGにおいてシステムズエンジニアリング手法に基づく障害診断のための「大規模・複雑化した組込みシステムのための障害診断手法～モデルベースアプローチによる事後V&V※1の提案～ Ver. 2.0」(事後V&V)と、この手法を利用する際のシミュレーション環境のための事後検証用サンプルシステムを報告書※2にまとめて公開すると共に、システム安全性解析手法WGを設置してマサチューセッツ工科大学(MIT)で提唱されている安全性分析手法STAMP/STPA※3について調査/試行し、入門書※4にまとめて公開した。

1　障害原因診断手法

1.1　背景と狙い

ハードウェアの性能向上とネットワーク化の進展により、組込みシステムは従来の単一装置による単独システムから複数の機器やソフトウェアが協調する複合システムになっている。複合システムでは必然的にシステム間インターフェースが必要となり、このシステム間インターフェースの増加が今日の組込みシステムをより複雑なものにしている。そのため、組込みシステムに事故が生じた場合、その原因調査は容易ではない。

大規模・複雑化した組込みシステムに発生する障害の原因を体系的に究明するには、設計段階における検証と妥当性確認(V&V)で用いられる方法論の考え方を用いることが重要である。

また、障害原因の究明を目指すだけでなく、社会的な責任の遂行のため、根拠に基づいて広く社会に合意されるような説明となる調査・分析が求められている。重要な制御ロジックとしてソフトウェアが含まれる複雑な組込みシステムでは、製造者だけによる原因調査では不十分であるという点も問題意識として持っている。

2015年度の活動では主に、要求仕様のモデル化による理解と障害原因の診断手法の検討や、2節でも説明するSTAMP/STPA手法の適用、Simulinkを用いた新たな事後検証用のサンプルシステムの開発について取り組み、それらの結果を事後V&V報告書の改訂版として取りまとめた。

1.2　事後V&Vの特徴

V&Vは設計段階での考え落としや実装ミスを防ぐ方法であるが、障害発生時の原因究明では、正に、これと同じことを行う必要がある。更に、抽出した原因仮説により、発生した障害から観測される事象すべてを再現できるという証明まで必要とされるため、設計段階でのV&Vよりも具体的できめ細かい方法論を確立しておく必要がある。図1は事後V&Vの体系をまとめたもので、各要素技術の概要は以下の通りである。

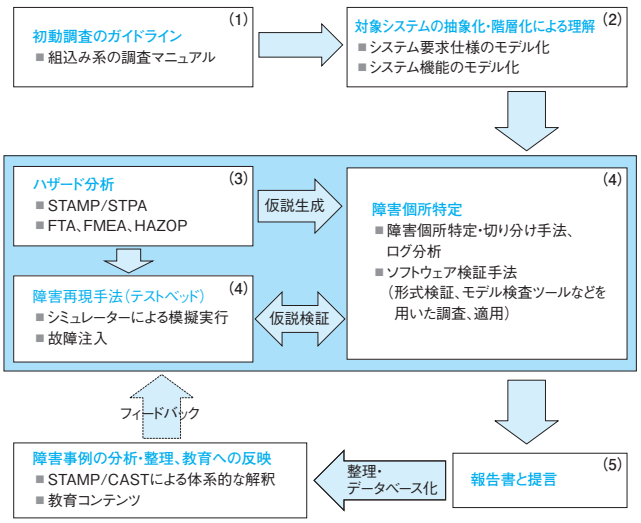

図1　事後V&Vの全体像

(1)初動調査としての分析に必要な情報の収集
(2)要求仕様障害発生に関連する部分の第三者による理解のための抽象化と階層化
(3)ハザード要因の体系的分析による障害原因仮説のリストアップ
(4)障害を引き起こすサブシステムの絞り込みと抽出した原因仮説の検証
(5)報告書へのまとめと本質的な改善に向けた提言

【脚注】
※1　Verification and Validation
※2　http://www.ipa.go.jp/sec/reports/20150331_4.html
※3　Systems-Theoretic Accident Model and Processes / System Theoretic Process Analysis
※4　http://www.ipa.go.jp/sec/reports/20160428.html

以下、今年度重点的に検討したシステム要求仕様のモデル化とSysML記述ツールを用いたSTPA分析、STAMPによる障害原因仮説の生成について概要を述べる。

1.3 システム要求仕様のモデル化

2014年度に事例とした化学プラントシミュレーターに関する要求をSysMLで記述し、STPAを適用して分析した。作業の手順と項目、SysML図との関連を表1に示す。

表1　システム記述に用いた作業の流れと内容

手順	作業項目	使用するSysML図
要求分析	要求を獲得する	要求図
	システムとその境界を決める	ブロック定義図
	システムの使われ方(機能)を定める	ユースケース図
	ユースケースの動作を表現する	シーケンス図 アクティビティ図 状態機械図
アーキテクチャー設計	システムを構成要素に分解する	ブロック定義図
	部品の相互作用を定義する	シーケンス図 アクティビティ図
	部品の相互接続を定義する	内部ブロック図
制約評価	システムの安全制約を獲得する	構造に関する図 動作に関する図
	ハザード分析し、設計を修正する(繰り返す)	
要求割当て	構成要素の要求仕様を定める	ブロック定義図
	要求の追跡性を確立する	要求図

STPAは、基本的にはシステム開発の初期の段階で、ハザードを引き起こす要因を識別することを可能にする。この手法が、既に開発を終えて稼働しているシステムに潜在する障害原因を識別することができるかを考察するために、SysMLで作成したシステム記述を参照し、以下のようにSTPA分析を進めた。

(1)コントロールストラクチャー図の作成
(2)非安全なコントロールアクションの識別
(3)ハザード誘発要因の識別
(4)安全制約の追加

このような分析により、診断対象とするシステムが得られた安全制約を守っているか、守っていないとすればその侵害によって障害現象が発生するか、といった仮説生成に活用できるものと考えられる。

1.4 SysMLとSTAMPによるシステム統合モデル化

前節ではSysMLの図を参照してSTPAを実施しているが、通常の開発工程とSTAMPに基づく分析工程の統合を図ることを目的に、SysMLの要求図を用いた安全制約の記述やSysMLのブロック定義図と内部ブロック図を用いたコントロールストラクチャーの記述を行った。

STPAの準備作業ではアクシデント・ハザード・安全制約の識別が行われ、図2に示すようにSysMLの要求図を用いてこれらの識別を実施している。(事例は前節と同様、化学プラントシミュレーターである。)

コントロールストラクチャーの記述においては、SysMLの内部ブロック図を用い、以下の手順で行った。

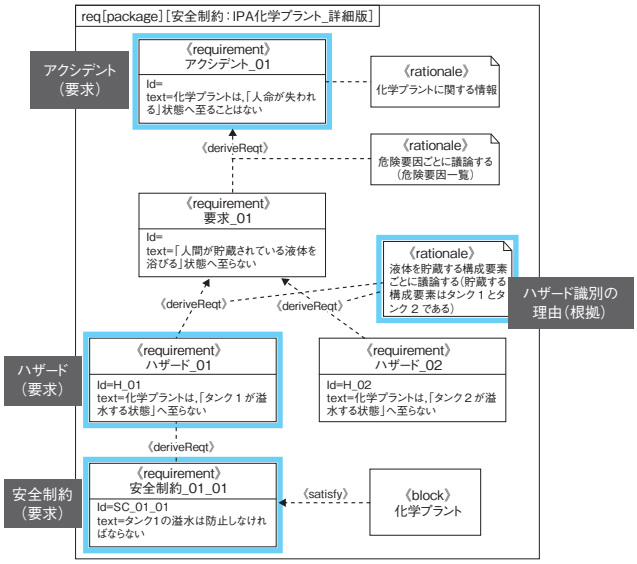

図2　要求図を用いたアクシデント、ハザード、安全制約の識別

(1)ブロック定義図(BBD)によってシステム構成要素を階層的に整理する
(2) BBD内でコントロールストラクチャー記述対象のブロックのレベルにそろえた内部ブロックを抽象コントロールストラクチャー(抽象CS)とする
(3)抽象CS内のブロックに対して内部ブロック図を記述し、そのレベルで得られたものを詳細コントロールストラクチャー(詳細CS)とする
(4)分析の観点に基づいて詳細CSのモデル要素を整理し、最終コントロールストラクチャーを構築する

両者の工程を統合することで、高機能なSysML記述ツールをSTAMPの構成要素の記述に利用でき、人手による作業と比較して作業効率が向上する。しかし、SysML記述のツールはSTAMPの構成要素記述やSTPA支援を目的としては作られていないため、今回記述したよりも抽象度の高いコントロールストラクチャーの記述法、記述した安全制約やコントロールストラクチャーに基づくSTPA支援の方法には更に検討が必要である。

1.5 STAMPによる障害原因仮説の生成

化学プラントシミュレーターに対してSTPAを適用して詳細な分析を行い、ハザードを誘発するシナリオを一般化し、運転員とコンピューターの間、並びに運転員とプラントの間のシナリオとしてまとめたものが図3である。

これらの誘発要因は応用領域によって異なるとはいえ、過去の事故原因を考えてみると一般的に成り立ち得る要因でもある。近年の組込みシステムではコンピューターを介した制御が一般的になっているが、このような制御では状態表示画面がコンピューターの不具合でフリーズした際に、それに気づかないこともあり得る。

安全が最重要視されるシステムでは、コンピューターが

ダウンした際の対処方法も設計に組み入れておくべきである。ここで示したようなハザード誘発要因をまとめておくことで、設計の際の気づきとして用いることもできる。

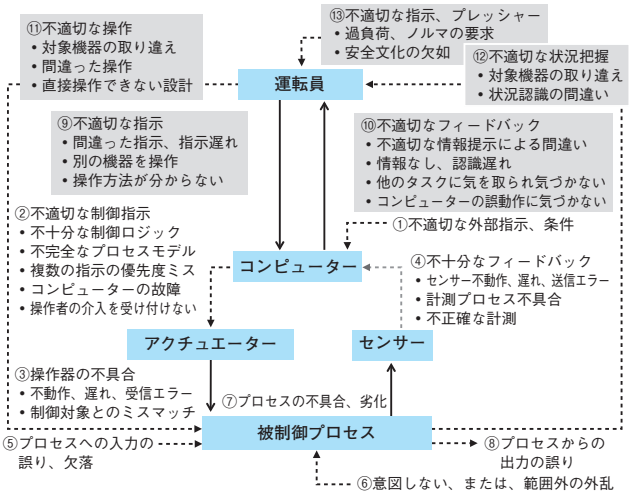

図3　人間系も含めたハザード誘発要因のまとめ

1.6　まとめと今後の取り組み

大規模・複雑化する組込みシステムが増えていく中で、その安全設計やトラブル対応には既存の技術では対応しきれなくなってきている。このようなシステムにおいて障害原因究明が必要とされた場合には、その障害の状況に応じて既存の技術だけでなく、STAMPのような最新の技術を迅速かつ適切に組み合わせて解決していくことが必要になる。

2015年度は化学プラントシミュレーターを仮想の対象として、様々な障害原因究明にかかわる要素技術の適用方法を検討した。要求仕様や機能仕様のSysMLを用いた記述法、SysMLとSTAMPを組み合わせた複雑なシステムのハザード分析、機械学習・人工知能技術を用いた障害診断法、形式手法（モデル検査）を用いた人間・機械の協調制御アルゴリズムの検証、などである。このように具体例でその使い方をショーケースのように可視化しておくことは、いざというときのための準備として必要不可欠なことであろう。

また、要素技術の検証のためのサンプルシステムとして、化学プラントシミュレーターに加えて倒立二輪車の自立制御と人間との協調制御システムを作成した。現実の世界の障害を直接扱うことは必ずしも容易ではないことから、今後も、これらのサンプルシステムを用いて、障害原因究明のためのツールの準備とその利用方法の蓄積を行っていく予定である。これは、障害診断にかかわるエンジニアの育成にも大きく寄与できると考えられる。

2　システム安全分析手法（STAMP/STPA）

近年、システムが大規模・複雑になり、更にネットワークによって相互に接続されて、システム障害もその構成要素に起因するのみならず、構成要素同士の間、更には、システムと人間との間の複雑な相互作用に起因するものがしばしば発生している。

このような状況において、SECではシステムの安全性に関して世界的に著名なMITのNancy Leveson教授が提唱しているSTAMP/STPAに着目し、前節の障害原因分析において適用を始めた。更に、この手法のより深い理解と有効性の確認、適用事例研究の実践などを当面の主な目的とするシステム安全性解析手法WGを設置し、活動を開始した。

STAMP/STPAは、FMEAやFTAをはじめとする従来の技術では全く達成不可能だった「ソフトウェアの仕様書なしにソフトウェアの安全解析を行うこと」、「故障にかかわらないハザード発生シナリオを識別すること」で、従来不可能と考えられてきた、「ソフトウェアの要求・設計ミスによるハザード誘発要因を識別する方法」と言われている。

2015年6月にはSEC特別セミナー「システムベースのエンジニアリング最新動向：複雑化するシステムの安全性とセキュリティを確保するためにすべきこと!」を開催し、Leveson教授に講演いただくと共に、STAMPの実経験者、研究者とWG委員を交えて「日本におけるSTAMP活用の仕方について」と題してパネルディスカッションを行った。併せてWG委員や関係者とLeveson教授との意見交換会を行い、STAMPの理解を深めることができた。

当WGの活動では、この手法に先進的に取り組んでいる委員の協力を受け、手法を理解する目的で委員から提供された具体的な事例（単線踏切制御システム）について、専門領域の知識の提供も受けながら、STAMP/STPAの適用研究を進めた。2016年1月に、国立研究開発法人宇宙航空研究開発機構（JAXA）とIPAとの共催で開催した第13回クリティカルソフトウェアワークショップ（13thWOCS[2]）においてもLeveson教授に特別基調講演をお願いし、それに引き続いてLeveson教授並びにJohn Thomas博士とWG委員及び関係者との意見交換会を開催した。

意見交換会において、Leveson教授より、上記踏切システムの事例が、初歩的な例ではあるが、対象システムのモデル化並びに安全性分析方法として良好であるとの評価を受けたこともあり、入門書「はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～」として小冊子にまとめて公開している。冊子の詳細な内容については本誌52ページの「システム理論に基づくアクシデントモデルSTAMP」を参照されたい。

引き続き人と機械が相互に関係するシステム、人と組織を中心とするプロセス、ITサービスなどの事例を分析しSTAMP/STPAの有用性を示すと共にHow toを事例と併せて示すことにより活用を促進していく。今年12月にはSTAMPワークショップinジャパンも計画しておりコミュニティ形成にも貢献していくことを目指している。

「はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～」