これからの複雑システムの安全分析STAMP/STPA

会津大学 名誉教授 **兼本 茂**

これからの複雑な工学製品では、人と高度なソフトウェアが連携・協調して高度な機能を提供することになるが、そこで期待されている新しい安全分析法STAMP/STPAの応用可能性を論じた。故障をなくすのではなく、安全を制御するというパラダイムシフトの重要さを指摘すると共に、複雑システムの安全論証のあり方を議論した。

1 STAMPと安全分析

MITのナンシー・レブソン教授は、その著書「Engineering a Safer World」の中で次世代の安全分析法の必要性を図1のような形で主張している[1]。今の製品開発、システム開発で用いられているFTAやFMEA、HAZOPといった安全分析法は、いずれも50年以上も前に開発された方法論であり、今のコンピューター制御が導入された複雑システムの安全を担保するには不十分であるということである。従来の安全分析法はコンポーネント故障が事故を引き起こすという仮定のもとで、その故障を最小化する信頼性工学に基づいた方法論であるが、複雑システムにおいては、コンポーネント間のコミュニケーション・ミスマッチが事故を引き起こしているという現実を考慮した安全分析が必要になる。

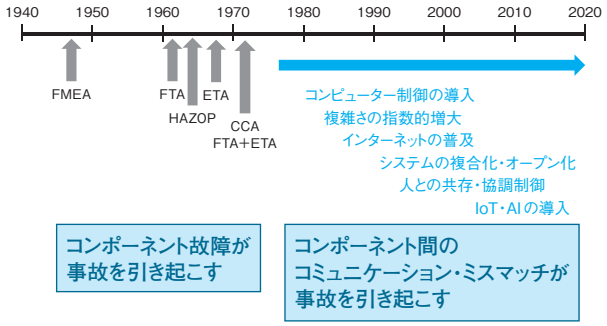

図1　工学製品開発の進展と安全分析時代変化

ナンシー・レブソン教授による講演[2]では、この製品開発の技術変化を、コンピューター制御の導入、複雑さの指数的増大、新技術の導入という3点で象徴しているが、これをもう少し具体的に記述したのが図1である。ここで言う複雑さの増大は、本質的には、そこで使われるソフトウェアの高度化、知能化に起因している。例えば、自動車やロボットのような製品のソフトウェアによる柔軟で知的な制御は、人との協調制御を可能にし、より安全なシステムを作ることができる。しかしながら、その一方で、人とソフトウェア制御のコンフリクトや相互作用のミスマッチが起きて、想定しなかったような事故が起こる可能性もある。

このような背景から、ナンシー・レブソン教授は、次世代の安全分析に用いる基本モデルとして、図2に示すようなSTAMP（System Theoretic Accident Model and Process）を提唱している。安全を制御するために、人やコントローラは被制御対象の挙動を示すプロセスモデルに基づいて、被制御対象に対して能動的な制御行動（Control Action、CA）を提供することで安全を確保する。また、CAの結果はフィードバック情報を通して認識し、その妥当性を評価する。この安全をCAによって確保する、更にはCAの乱れが事故を引き起こすという考え方は、従来のコンポーネント故障が事故を引き起こすという信頼性工学の考え方と本質的に異なるパラダイムシフトであり、福島原発の事故後に注目されているレジリエンス工学とも相通じるものである。人と高度ソフトウェアを内包する複雑システムにおけるエラーやコミュニケーション・ミスマッチは完全には避けることができないものであり、その影響を最小限にとどめたり、更には、最悪の事態を防いだりするためのCAが重要であるというメッセージでもある。

既にソフトウェアを用いた安全の制御は広く用いられるようになっているが、これらの多くは従来のフェイルセーフなどの機械安全技術の置き換えであって、IEC61508などの国際規格

によりその開発プロセスを保証することで信頼性を確保している[3]。一方で、通信ネットワーク、センサ技術とソフトウェアの組み合わせで、大規模化、複雑化、高度化（人工知能など）が始まり、規格の範囲を越えて人間と機械の協調制御によって安全を守る時代にもなっている。中村教授は、それを協調安全と称して、Safety2.0という次世代の安全の考え方を提唱している[4]。「協調」という概念は二つの独立した主体の協力関係を示しており、どちらが主（制御主体）でどちらが従（被制御主体）かという視点でのあいまいさは残るが、ソフトウェアの高度化で状況に応じて主従を切り替えるような柔軟な安全制御機構が可能になると考えられる。しかしながら、このような協調安全によって複雑システムの安全をどのように論証するかはそう簡単ではない。

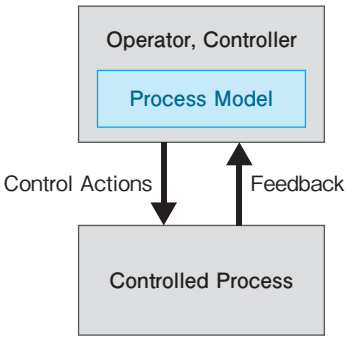

図2　STAMPの基本モデル

現状の安全クリティカルシステムにおけるソフトウェアの安全規格IEC61508やISO26262では、人と機械の協調制御や人工知能のような高度なソフトウェアによる安全の確保は言及されていないが、上述のように、人と高度なソフトウェアを含んだ今後の複雑システムの安全設計の問題にも正面から取り組む必要が出てくると思われる。このような状況の中で、STAMPをどう活用していくかは喫緊の課題と言える。ナンシー・レブソン教授によると、複雑システムの安全は創発特性を持っており、構成要素であるコンポーネントの安全制約を守っていれば、システム全体の安全を守れるものではないと言われている。システムの振る舞いを、個々の要素に分解して説明する信頼性工学的手法、還元主義的手法では複雑システムの安全は確保できないという主張であるが、創発特性をそのままにしておいては、複雑システムの安全な設計はできない。もちろん、工学システムに「絶対安全はない」というのも事実ではあるが、エンジニアとしての知見をより広く集めて、より安全なシステムを作るための方法論を探ることが本稿の目的になる。

2　安全論証としてのSTAMP/STPA

上述のSTAMPに基づく安全設計や事故分析の手順として、ハザード分析法STPA（System Theoretic Process Analysis）や事故分析法CAST（Causal Analysis based on STAMP）といった方法論が提案されている。また、米国、欧州、日本で、STAMPワークショップが定期的に開催され、多くの産業分野での応用事例が報告されている。しかしながら、これからの複雑システムの安全設計プロセスにこのSTPAやCASTをどのように取り込んでいくかはまだ手探りの段階であると言うべきであろう。

これまでの大規模な工学システムの安全設計は、FTA、FMEA、HAZOPのような信頼性工学方法論でなされているが、設計時に想定していない環境変化や運用のされ方、更には仕様書そのものの欠陥によって事故が起こっているのも現実である。事故の後には、事故調査委員会等で原因の究明がなされ、更には、水平展開といった形で対策が取られているが、このような安全管理・対策は、事後に行うという意味でリアクティブな安全論証と呼べる。想定外の大きな地震と津波により引き起こされた福島の原発事故は、その後の安全規制のあり方まで大きく変えたが、これがリアクティブな安全論証の典型と言える。しかしながら、そこには、事故の後に初めて気づいた知識である「後知恵」が必ず含まれる。一方で、もし、先に述べた創発特性を持ったハザードを事前に予測して設計に反映できるとすれば、これは、プロアクティブな安全論証と言うことができよう。そのための具体的な安全論証法として、STAMP/STPAはどのように役立てることができるのであろうか？

IEC61508やISO26262などの国際規格では、安全クリティカルシステムの適用範囲を総合的に定義した後、そこにあるハザードとリスクの評価（Hazard Analysis and Risk Assessment, HARA）を行い、更には、安全整合性水準（SIL/ASIL）を割り当てた上で安全要求事項の仕様を作成して詳細設計に入る。SIL/ASILの評価では、ハザードの深刻度、曝露確率、回避可能性を見積もるといった手順が必要である。これらの一連の評価手順が安全論証と呼ばれるが、人や人工知能のような高度なソフトウェアが入った複雑システムは対象外とされている。ここで期待されているのが、新しい安全分析法としてのSTAMP/STPAである。

図3は、複雑システムの創発的な安全特性を、ナンシー・レブソン教授の考え方に著者の解釈を加えて象徴的に示したものである。個々のコンポーネントの安全制約だけではシステム全体の安全制約に漏れがあり得ること、更に、その周囲に想定外の

環境変化による危険が潜んでいるという二つの重要な論点を示している。STAMPの最大の特徴は、図2に示したような制御主体と被制御主体の相互作用の抽象モデルである。この図は簡単化し過ぎてはいるが、これらを階層的に積み重ねていくことで、複雑システムの安全制御機構を第三者にも理解可能な形で可視化することができる。抽象化と可視化が複雑システムを理解する唯一の方法であるというのがナンシー・レブソン教授の格言でもある。このようなモデルに基づいた分析により、上述の最初の論点である複雑システム全体に網をかけるようなシステム安全制約を導出することができる。この安全制約を網羅的に導出するために、STPAでは、図4に示すような4つの非安全制御行動（UCA）を用いる。これは、Step-1の手順と呼ばれ、UCAごとに、図2のSTAMPモデルを用いて、それがどのようなハザードにつながるかのシナリオを導出していく。これは、従来法との対比で言えば、FMEAに似た推論法になる。ここで安全論証として大事なことは、安全制御行動（CA）とその結果として観測されるフィードバック情報を明示化しておくことである。また、CAの決定に必要なプロセスモデルや外部環境要因も第三者にも分かるような形で表現しておく必要がある。これらの情報があいまいであると評価者によってハザードに至るシナリオが異なってくるためである。このUCAが決まれば、Step-2の手順の中で、UCAを引き起こすハザード誘発要因・シナリオを、STAMPモデルの因果関係を逆向きにたどりながら導出し、更には、それらの要因を防止するためのコンポーネント安全制約を導出していく。

もう一つの論点である想定外の環境変化によるハザードについても、制御構造図のプロセスモデルの中で外部の環境変化も明示化してUCA分析をすることで、複数のレビュアによる相互の議論を行うことができる。想定外というのは、設計に携わるエンジニアの知識や過去の経験に大きく影響されるわけであるが「ある人の想定外は、ほかの人にとっては想定内であり得る」という現実に目を向けた安全設計の相互レビューにより、この想定外をより少なくすることが期待できる。先に述べた東日本大震災の際にも、悲惨な事故にあった福島第一原発と同時に、同じ地震と津波の影響を受けながら、これを乗り越えて安全を

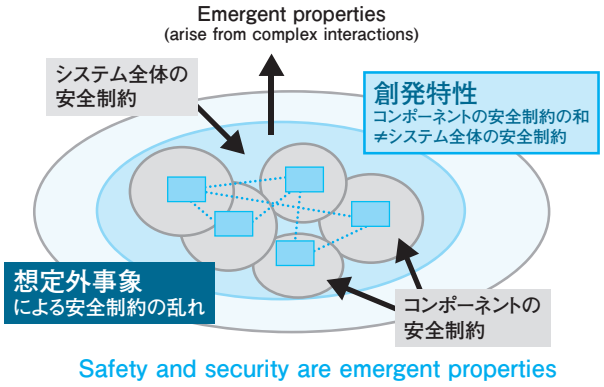

図3　複雑システムの安全と創発特性

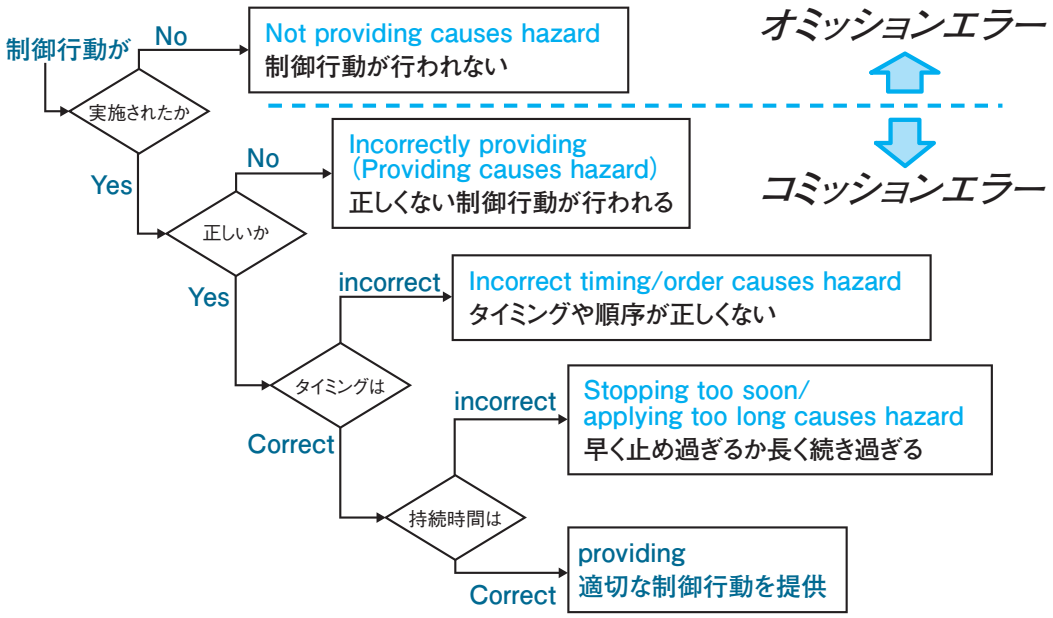

図4　非安全制御行動（UCA）の分類

表1　従来の安全分析法とSTPAによる安全分析法の特徴の比較

手法名	分析方法	特 徴
従来手法 （FTA、FMEA）	●FTAは望ましくない事象をゴールとして、その要因をツリー状に展開・分析して故障要因を分析する ●FMEAは、構成要素に起こり得る故障モードを予測し、考えられる原因やシステム全体への影響を解析・評価する方法 ●システムの構成要素と故障モードが決まるアーキテクチャ設計の段階から適用できる	●構成要素の故障が事故を引き起こすと考え、その故障を最小化する信頼性工学的手法 ●ドミノモデルやスイスチーズモデルといった故障の一方向への伝搬モデルに基づいて、故障の因果関係を分析する ●故障要因に故障確率を割り当てることで定量的な故障分析ができる ●人や複雑なソフトウェアの相互作用を伴う複雑システムの故障分析では、すべての故障モードを拾い出すことが難しい
STAMP/STPA	●アクシデント、ハザード、安全制約に基づき、安全制御構造図を明示化（Step-0） ●４つの非安全制御行動（UCA）に分類してハザードへの影響を分析し、安全制約を詳細化（Step-1） ●非安全制御行動を引き起こすハザードシナリオを、制御構造図と経験に基づくヒントワードを用いて分析（Step-2）	●故障を低減するという信頼性工学的手法ではなく、事故を回避するための制御行動の乱れを分析する安全制御工学的手法 ●安全を確保するための制御行動とそのフィードバックという動的システムの中で事故が起こるというモデルに基づく ●抽象化・階層化したモデルで複雑さを理解するトップダウンのシステム工学的手法で、人・組織や複雑なソフトウェアの相互作用の不具合に伴うハザードを分析する ●安全制御構造が可視化でき、第三者を含む複数の専門家によるレビューがしやすい。抽象化・階層化したモデルなのでドメイン知識の少ない人でもレビューに参加できる ●解析する人の能力への依存度が大きい

保った女川原発や福島第二原発は、想定外へ対処できた良好事例として参考にすべきものであろう。

上述の一連のSTAMP/STPAのハザード分析手順は、従来のHARAと比べると、リスクの定量評価をせずに、ワーストケースで見積もるという違いがあることに気づくが、本質的な違いはないと言えよう。手法としての特徴は、網羅性を持ったUCAという行動に着目して、それがシステム安全に与える影響と、UCAが引き起こされる要因を分析するということである。

以上の議論をもとに、従来の安全分析法とSTAMP/STPAの特徴を比較して表1にまとめておいた。定性的な比較ではあるが、STAMP/STPAの事例を見る際の参考にしていただきたい。

3　まとめ

本稿では、抽象的な表現ではあるが、これからの複雑システムの安全分析のためにSTAMP/STPAをどう活用するかを論じた。STPAは下記の観点から今後の活用が期待されるが、本シリーズの別稿のような具体的な事例で理解を深めていく必要がある。

(1) 抽象化・階層化したSTAMPという安全制御構造モデルでシステムを明示化して、複雑さに惑わされることなく、システムとコンポーネント安全制約を考える。

(2) トップレベル安全制約からトレーサビリティを持ってコンポーネント安全制約を導くことで、運用後の更新まで含めた安全論証に役立てる。

(3) 多様な環境・コンテクストのもとで、第三者レビューも含めて想定外のハザードも発想して安全制約を立てる。また、本稿では論じていないが、複数の制御主体と複数の被制御主体の中で、CA相互のコンフリクトが起こったり、制御主体と被制御主体の逆転が起こったりする際の安全評価にも、可視化された安全制御構造図は役立てることができる。

引用文献

[1] Nancy G. Leveson :Engineering a Safer World :Systems Thinking Applied to Safety (Engineering Systems), The MIT Press, 2012.
[2] 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、2015年6月18日、https://sec.ipa.go.jp/seminar/20150618.html
[3] JASA安全性向上委員会編・著：組込み技術者のための安全設計入門、電波新聞社、2010年
[4] 日経BP「Safety2.0」http://www.nikkeibp.co.jp/atcl/column/16/safety2/