SEC 特別セミナー「Engineering a Safer World」について

独立行政法人情報処理推進機構（IPA）
技術本部 ソフトウェア高信頼化センター（SEC）ソフトウェアグループ リーダー
中村　雄三

1. はじめに

近年、システムの複雑・大規模化に伴い、システムの安全性を確保することがより重要になっている。そこで独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア高信頼化センター（SEC）では、2014 年 1 月 21 日に、マサチューセッツ工科大学のナンシー・レブソン教授と有人宇宙システム株式会社の星野伸行主幹技師を招いて特別セミナー「Engineering a Safer World ―安全なシステムを実現するための新たなアプローチ（手法と事例）―」※1 を開催した。

ナンシー・レブソン教授（以下「教授」と略す）は、安全なシステムとソフトウェアを目指した研究の第一人者であり、国内では「セーフウェア」の著者としても著名な方である。今回のセミナータイトルは、最新の著作「Engineering a Safer World」※2 からいただいたものであり、講演では著書の中で新たに提唱されている「システム理論に基づく事故モデル（STAMP※3）」、「STAMP に基づく安全解析手法（STPA※4）」、及び「STAMP に基づく不具合分析手法（CAST※5）」を中心に事例を交えてご講演いただいた。また星野主幹技師には、STAMP/STPA の概要を補足していただくとともに、宇宙機における実際の適用事例に関してご紹介いただいた。

2. Engineering a Safer World（ナンシー教授）

ここでは教授の講演の主なポイントを概説する。

「安全」と「信頼性」は異なる

システムを構成する個々のコンポーネントの信頼性が高くても事故は起こりうる、逆に個々のコンポーネントの故障があっても事故につながるとは限らない。最近の事故は、コンポーネント間の相互作用によるものが多く、システム全体の安全性とそれを構成する個々のコンポーネントの信頼性は別物、つまり個々のコンポーネントの信頼性を上げたからといっても、システム全体が安全とはいえず、システム全体にわたる安全性の考慮が重要である。

例えば、ソフトウェアが要件通りに極めて高い信頼性で開発されたとしても、システム安全に関する要求の欠如、或いは特定の動作条件に関して要件で規定されていない場合には、安全とは言えない。

従来の「安全工学」、「信頼性工学」の問題

従来の安全工学、信頼性工学は、コンピュータが普及するはるかに前に考案されたものであり、比較的単純な電子機器システムを対象にしていた。しかし近年は、あらゆるところにコンピュータ制御が入り、システムが大規模・複雑化してきており、従来の手法では安全に対する対応ができなくなっている。例えば、操作者の役割も、装置を直接制御する事から、装置を制御するコンピュータを監督する、というように変わって来ている。また、システムが単純な頃はほぼすべての試験が可能であったが、システムが複雑化したことによりすべてを試験することが難しくなっている。

このような中で、個々のコンポーネントの不具合ではなく、システムの上位レベルの設計上の誤り等により事故が発生する事、システム全体が複雑化し、人間が全体を把握し制御することが難しくなっているにもかかわらず、何かあるとシステム設計上の問題ではなく操作者に責任を負わせようとする傾向がある、といった状況になったため、これに対処できる新たな方法論が必要となった。

従来の「事故モデル」の問題

事故モデルには 2 種類が考えられる。①単一、または複数のコンポーネントの不具合から生じるもの、②コンポーネント間の相互作用により生じるもの。近年では、コンピュータやソフトウェアが導入され、コンポーネント間の密接な結合や複雑な相互作用により、②に起因する事故が増えている。このような事故に関しては、従来の「複数の原因の連鎖による事故モデル（ドミノモデル）」

【脚注】
※ 1　http://sec.ipa.go.jp/seminar/20140121.html
※ 2　http://mitpress.mit.edu/books/engineering-safer-world
※ 3　STAMP：System-Theoretic Accident Model and Processes
※ 4　STPA：System-Theoretic Process Analysis
※ 5　CAST：Causal Analysis using STAMP

で捉えようとすると限定的になるため、全体を見て原因になりうるすべての要因に焦点を当てるべきである。

システム理論に基づく新たな事故モデル（STAMP）

事故は、複雑で動的なプロセスにかかわるため、従来のようなシステム内での単純な不具合イベントの連鎖ではなく、システム、操作者、環境も含めた相互作用の中での動的な制御の問題として捉える。システム全体に対して安全を確保するためには、安全のための一連の制約を実施する必要がある。事故は、システムコンポーネント間の相互作用が、この制約を乱した時に発生するものと考える。安全でない制御動作は以下の 4 種類に分類される。①安全のために必要な制御コマンドが送出されない、②安全でない制御コマンドが送出された、③基本的に安全なコマンドの送出が早すぎた／遅すぎた、④制御の停止が早すぎた／長すぎた。このように安全性の確保とは、信頼性の問題ではなく制御の問題である。従って、安全に関する従来との違いは、「不具合を防止する」のではなく、「システムの振る舞いの中で安全のための制約（safety constraint）を確実に実行する」ということになる。教授はこの点に関して、講演では幾つかの事例を挙げて説明された。

さらに、従来の観点では、操作者のミスに起因した事故に対して、対策として①さらに自動化を進める、②ルールや手続きで厳しく規制する、との考え方であった。一方、新たな考え方では、操作者のミスは原因ではなく、全体システムの設計を見直すべき兆候（symptom）と捉えている。

STAMP に基づく安全解析手法（STPA）、及び STAMP に基づく不具合分析手法 (CAST)

ここでは誌面の関係で、STPA、CAST の手法の内容に関しては説明を省略する。教授は毎年、STAMP ワークショップを開催されており、これらの手法の適用事例が数多く集まっているとのことであった。実際に、航空機、宇宙機、航空管制、自動車、化学プラント、原発等の分野に適用されているとのこと。それらの経験から STPA に関しては、従来の FTA、FMEA 等の手法と同等以上のハザードを、しかも従来よりも少ないコストで実施できた、と報告されていた。

教授の講演に対する主な質疑応答として、一つは従来の手法から新たな手法に切り替える判断をどうしたらよいかの質問に対しては、比較的小規模からの試行適用が良いのではないか、もう一つは現時点での手法適用が専任の操作者を前提とした化学プラント等の産業界での分析が中心になっているが、一般利用者を対象とした場合どのような違いがあるかに関しては、現在、自動車メーカー等と検討を進めている、との事であった。

3. 宇宙機での事例紹介（星野主幹技師）

続いて、有人宇宙システムの星野主幹技師による STPA 適用事例の講演があった。今回の事例では、システムの IV&V（独立検証及び有効性確認）で検証対象を絞るため、ハザード解析技術として STPA を FTA 等と併用、不具合分析技術として CAST を他の技術と併用されているとのことであった。星野氏はまず STPA に関して実際の適用の流れを説明されるとともに、宇宙機 HTV(コウノトリ) での適用事例に関して紹介された。

特徴的であったのは、STPA により従来手法である FTA では識別されなかった幾つかの要因が検出された点であった。さらに、最近の取組みとして、操作者に関してヒューマンメンタルモデルを考慮した分析手法の紹介もしていただき、非常に興味深いものであった。

4. おわりに

教授の日程調整等のため、特別セミナー開催の周知が年末になってしまったにもかかわらず 200 名近い方に参加いただき、活発な質疑応答も行うことができた。両氏の講演は、今後の大規模・複雑化する製品・システムの安全を考える上で、極めて参考になるものと考える。また STAMP/STPA,CAST に関しては、国内ではまだ適用事例が多くないと考えられるが、今後、試行評価等が進められ、安全のために寄与する事が期待される。

最後に、このセミナーのために来日いただいたナンシー教授、及び多忙な中で講演いただいた星野主幹技師に感謝したい。