これからのシステムの安全・安心

～世界のシステム開発方法論のトレンドから思うこと～

慶應義塾大学大学院システムデザイン・マネジメント研究科 准教授
白坂　成功

1 はじめに

日本は大変信頼性の高い製品を作り出し、高品質なものづくりで一躍世界的な工業国となった。そして、日本のものづくりの精神は、昔から変わらず今も引き継がれていると考えられる。一方で、世の中はものすごい早さで変化を遂げてきた。まず最初に変化したのが、製品のソフトウェア化である。高度にソフトウェア化された製品では、たとえ高い信頼性を持っていても、決して安全ではないことを MIT の Nancy Leveson 教授がその著書「Safeware」で広く世に知らせた。その本では、ハードウェアの偶発故障という予見可能性の高い故障モードに基づく安全性解析では対応できない、ソフトウェアのシステム故障という予見可能性の低いものに対応せざるを得ない難しさを指摘している。

では、これからのシステムの安全性はどうなるのであろうか。ここでは紙面制約の関係から既にその傾向が現れ始めている三つの可能性を述べてみたい。三つとは、対象範囲の拡大と複雑化、ライフサイクルのカバー範囲の拡大、より複雑な設計の必要性である。また最後には、どのような人がこういったことに対応可能なのか。人材育成の観点から述べてみたい。

2 対象範囲の拡大と複雑化

これまでは単一のプロダクトあるいはシステムについての安全性のみを考えれば良かった。ところが現在では、当初つながることを想定していなかったシステムがネットワークを経由して論理的にも物理的にもつながるようになってきた。こういったものを扱う考え方として System of Systems（以降、SoS）という概念がある。米国の政府系コンサルティング会社である Aerospace Corporation の副社長であった M.W.Maier 博士が 1998 年に INCOSE（International Council on Systems Engineering）のジャーナルで発表した「Architecting principles for systems-of-systems」によると、System of Systems（システムオブシステムズ）とは、その構成要素のそれぞれが独立したシステムとして扱えることができ、運用の独立性と管理の独立性があることと言っている。運用の独立性とは、それぞれが独立して利用されることを意味し、管理の独立性はとはそれぞれが別の組織によってそのライフサイクルが決められていることを意味している。実際に、自動車が家庭用の電力網に接続する例などは正に典型的な SoS であると言える。今後、IOT（Internet Of Things）が進むと、ますます SoS が身近に増えていくと考えられる。では、こういった SoS 全体の安全性はどのように実現すれば良いのか。未だ確定した方法は存在していない。最新の事例では、全体のアーキテクチャを高い抽象度で設計し、安全性にかかわる機能配分とインターフェースのみを規定して対応しようとしている。しかし、このアプローチでは決して安全性を

確実に保証してくれるものではない。今後、より確実な方法論が必要となるはずである。また、安心の観点では異なったアプローチが必要となると考えられる。つまり、安全を100％保証できないという前提に立ち、安全を保証できる範囲では積極的に安心感をあたえるだけでなく、安全を保証できる範囲を逸脱する場合には積極的に安心感をなくすことも必要であると考えられる。どのようにすれば人は安心し、どのようにすれば人は安心しないのかを明確にし、積極的に活用しなければならない時代がきていると思われる。

3 ライフサイクルのカバー範囲の拡大

２節では、対象の物理的な広がりについて述べた。ここでは、対象の時間的な広がりについて述べる。この時間的な広がりには２つの意味がある。一つは安全性を考慮しなければならない範囲が時間的に広がっているということである。もう一つは、かなり早いフェーズで安全性を考慮しなければ、安全性を担保することも、安全性を説明して安心感を得てもらうことも難しくなってきているということである。

具体的には、単に利用しているフェーズというだけではなく、利用中に使用環境やビジネス環境がかわったり、それにより当初想定していなかったものがつながるようになるなど、これまでは考えていなかったような単に「利用する」といった状況の先まで考える必要がでてきた。更に、２節で説明したように、全く違う管理のシステムがつながるSoSでは、SoSの全体構造を考えるときに安全性の考え方をいれておかないと、後から追加することができなくなる。ある単独システムの要求を決める段階（つまり、一つ上のシステムであるSoSレベルシステムのアーキテクチャ設計段階）において、安全性を埋め込まなければいけなくなってきた。更に、安全であることを伝えるためには、トップダウンで安全性を説明できなければいけなくなる。日本の多くの製品は、「あれは大丈夫か？」、「これは大丈夫か？」と聞かれると、ほぼ間違えなく大丈夫な設計ができている。しかし、「なぜ安全ですか？」と聞かれると論理的に説明できない場合が多い。これは、何が安全でない状態で、それがなぜ発生する可能性があり、その可能性すべてがきちんと対応されているということが説明できないからである。現在のシステム開発では、一つの分野・会社でやめることなく業務を続ける日本人のような場合、経験的に安全設計を実施することが可能である。しかし、今後、SoSのように、全く異なるシステムがつながるようになると、必ずしもこれまでの経験だけで対応可能であることが保証できなくなってくる。このような場合の対処としても、トップダウンでのリクス駆動の安全設計の考え方を入れざるを得なくなってくる。またそれを明示的に説明するための手法も重要となると考えられる。

4 より複雑な設計の必要性

上記のように物理的に、かつ時間的に俯瞰性を高めていっても、それだけでは実際にシステムを実現できなくなってくると考えられる。それは、人の認識できる範囲を超えた対応が必要となる場合が多くなると考えられるからだ。例えば、自動車ひとつをとってみても、急激な複雑さの増加のため、故障時の対応について、ドライバーが対応できないものが増えてきている。更に、自動化が進むに従って、機能のクリティカルさが増大し、瞬時に対応することが求められるようになっているからである。このようなことに対応する方策として、宇宙開発の分野では古くから利用されているFDIR（Fault Detection, Isolation and Recovery）という考え方がある。これは、宇宙システムが、オペレータが常に見ていられない（むしろ、見えてる時間のほうが短い）状態で、何か故障が発生しても宇宙システムが使えなくならないようにするために、自動で故障を検知し、それを分離し、そして再構成をするための設計の考え方である。これには、新しい技術が必要というわけではなく、新しい設計の考え方が必要となると思ったほうが良い。実際に、自動車OEMの数社が既にこの考え方を宇宙開発分野から学び、活用を始めている。今後は、３節で説明したことに対応するために、ますます広い分野でFDIRの考え方が使われると考えられる。

筆者は、宇宙ステーション補給期の開発において、確実に安全なシステムを実現するために、この FDIR という考え方を更に進めて、同時二故障の対応も実現した「階層化 FDIR」という新しい考え方を導入した。これは、FTA（Fault Tree Analysis）をベースに、故障に対するレスポンスと、対応可能な故障モードのカバレッジとの関係に目を付け、高レスポンスと低カバレッジの FDIR では故障が起きてから、その影響が波及するまでの間に FDIR で対応することで、ミッションの継続性をめざし、低レスポンスと高カバレッジの FDIR では、故障が発生してからの影響は波及しているが、大きなカバレッジをもった FDIR で確実に安全化を行う考え方を階層的に組み合わせ、想定可能な故障に対するミッション継続性と、想定ができない故障に対する安全性の確保を両立するために実施したものである。ただし、このような考え方は、その十分はシステムリソースを活用して始めて実現されているものであるので、低コスト化が求められるシステムにおいては、そのまま適用するのではなく、より工夫を凝らした実装が必要になることが考えられる。しかしながら、このような考え方はこれからの民生品開発においても多用されてくるであろう。

5 今後必要となる人材

上記のようなことに対応できる人材は、正に筆者が 2014 年の IT 白書に述べたようなシステムズエンジニアリング人材であると考えられる。そのような人材のとても重要な素養として、「色々なことに興味を持つ」ことや「より深く知りたいと思う」ことがあげられる。２節で述べた通り、これからのシステムは多様なものが相互につながるようになってくる。このときに、つながるものがどのようなものかを興味をもち、深く知っていくことは、幅広いドメイン知識を得るためにも欠かすことができない素養となると考えられる。更に、これらを扱うための方法論もますます進化していくと考えられ、それらを自ら見つけ、積極的に身につけていくエンジニアが必要となってくる。また、高い科学的スキルと創造的スキルを併せ持つことが必要となってくる。空間的にも時間的にも広がるシステムを適切に分析し、分解し、扱っていくことは高い科学的なスキルを持たずして行うことができない。また、初期のフェーズにおいて、広大な解空間から適切なソリューションを考えだすことは、正に創造的スキルが必要となってくる。これら科学的スキルと創造的スキルの両方を併せ持つ人材こそが、これからのシステムの安全・安心を担うことのできる人材となると考えられる。もちろん、このどちらも後天的に身につけることが可能であることは重要なポイントである。これまで強く求められてきた科学的スキルに追加して、これまではあまり明示的には言われてこなかったが、実際には設計作業の中で活用してきていた創造的スキルを積極的に身につけるように意識することで、これらの２つのスキルを強めていくことができる。それこそが、これからの若いエンジニアに求められることであると考える。

6 最後に

現在のシステム開発方法論の研究トレンドから、これからのシステムの安全・安心がどのようになっていくのか、三つの可能性を述べてみた。また、そういったことに対応できる人材とはどういう人なのかについても、その理由と共に簡単に示した。

私は、ドイツで欧州連合の会社で２年間働き、システム開発を通じて長年米国企業とつきあってきた。その個人的な感想からすると、世界で最も平均的に優秀で、勤勉なエンジニアは日本のエンジニアであり、適切な環境で適切な努力さえすれば最も結果をだすことができ、今後のシステム開発をリードできると心から感じている。逆に言うと、現在は、環境が適切ではなく、努力も残念ながら必ずしも適切な方向ではないのではないかと感じている。我々、大学という教育の場におくものは、この適切な環境を用意することに注力するので、ぜひ興味を持った方は適切な努力をしていただき、今後の社会を支えるシステムの開発に従事していただき、よりより社会を実現していただきたいと切に願っている。