IoT時代の安全安心に向けて

大規模・複雑システムの障害原因診断手法

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

システムの障害が社会に大きな影響を与える可能性が広がっており、コンピューターによる複雑な制御機能を持つ大規模システムの障害原因を迅速に追究し、再発防止のための提言を行う体系が必須となっている。この課題に対処するべくIPA/SECでは、2014年度より「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」の確立を目指して活動している。

1 障害原因診断フレームワークの確立

本活動では、システムのソフトウェアと付随するネットワークコミュニケーションの障害に注目し、それらの原因追究と解決への提言を行う方法論として、図1に示す構成の「事後Verification & Validation（V&V）」という考え方と、その要素技術を提案してきた。V&Vは要求仕様や設計の不備をレビューする視点で作られた体系であるが、設計時点での想定不足が運用後の障害を引き起こすと考えられることから、障害の原因診断にも使えるとして「事後V&V」と名付けている。設計・実装のミスだけでなく、要求段階の仕様ミスや市場での運用ミス、環境変化への対応ミス、セキュリティアタックによる侵害など多様な原因があるので、このような体系的な考え方が必要となる。

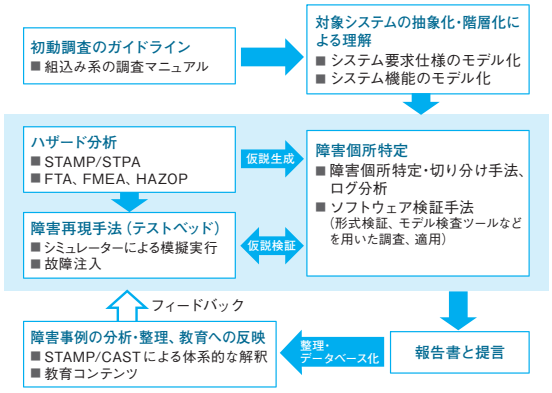

図1　事後V&Vの全体像

2 要素技術の展開

2014年度は、事後V&Vの全体像と既存技術として、その中で用いられる要素を紹介し、2015年度に、ハザード分析手法と原因個所の絞り込みについて具体化し、2016年度は比較項目や事例の追加で検討を深めた。

対象システムのモデル化ではSysML※1などのツールとの連携を含めてSTAMP/STPA※2手法を詳細検討し、2016年度はHAZOP※3との比較も行った。また、障害原因の仮説の絞り込みとしては、予兆監視にビッグデータを応用する事例、モデル検査を適用して要求仕様の不備を導く事例を報告した。

また、これら要素技術の検証・確認用のサンプルシステムとして、2014年度には化学プラントシミュレーター、2015・2016年度では倒立二輪車の制御システムを開発し、一般に利用できるよう公開した。

3 まとめと今後の取り組み

近年の大規模・複雑システムの障害は、開発時の既存V&Vをすり抜けて起こるものや運用後の環境変化への適応不足によって起こるものなどがある。これらの原因を究明する魔法の杖があるわけではないが、V&Vの考え方に基づいて、障害が起こった後に第三者の立場でシステム設計を再検証する方向性は妥当であろうと考える。

化学プラントシミュレーターや二輪倒立ロボットの模擬事故を事例としたが、人間と機械の協調制御で使われる製品やシステムが今後ますます増える状況にあり、このようなシステムのハザード分析の検討（図2）を通じて従来手法の限界と本活動による新しい手法の可能性が得られた。

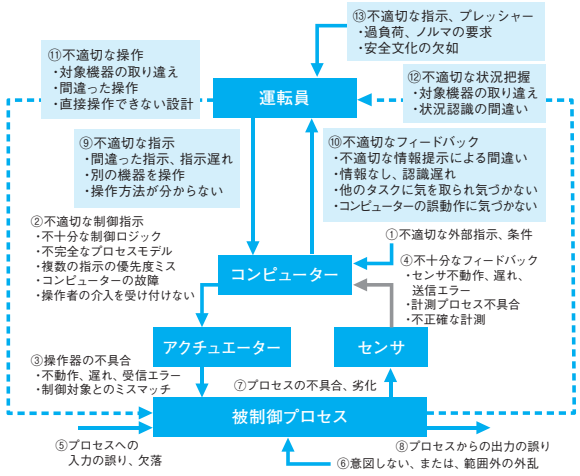

図2　人間系を含むハザード分析のガイダンス

今後、オープンエンドなシステムの安全性担保のため、解析手法への要請がますます高まる。STAMP/STPAの解析能力拡大のため、ヒューマンファクタや組織要因を取り込み、またレジリエンスエンジニアリングを活用することで、本活動をシステム安全性向上技術へと展開していく。

脚注

※1　Systems Modeling Language
※2　STAMP（Systems-Theoretic Accident Model and Processes）：システム理論に基づくアクシデントモデル
STPA（System -Theoretic Process Analysis）：STAMPに基づくハザード分析手法
※3　Hazard and Operability study