システム連携時のアクシデント要因を設計モデルの活用で効率良く洗い出す分析手法

Method to Clarify Causes of Accidents during Collaborative Operation between Different Systems through Effective Utilization of Design Modeling

MBSEによるシステム設計モデルを活用し，安全分野の分析手法と融合してアクシデントの要因分析を支援

より良い価値の実現に向けて，これまではつながりのなかったシステム同士でも連携が必要となる状況が増えています。この連携の不備が重大なアクシデントにつながる場合もあり，アクシデントの要因を洗い出し，対応策をシステム設計に反映する重要性は増しています。

そこで，システム全体を捉えて設計を行うMBSE（Model-Based Systems Engineering）の技術と安全分野の分析手法及び関連するノウハウを融合することにより，アクシデントの要因の洗い出しを効率良く実施し，開発の上流から品質を確保する仕組みを構築しました。

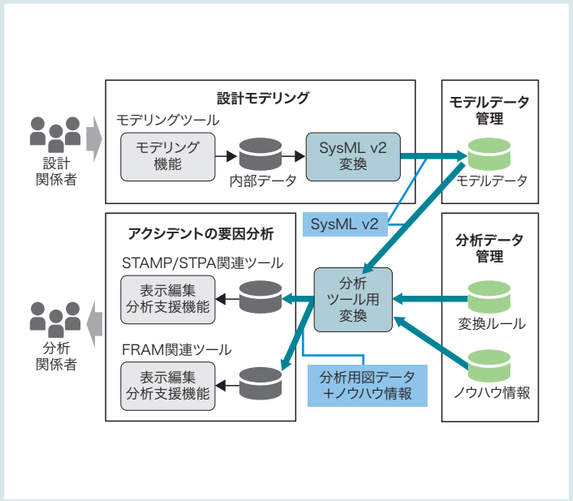

図1．設計モデリングとアクシデントの要因分析のデータ連携
SysML v2により設計情報を共有することで，正確かつ活用しやすい設計データ形式での要因分析環境を容易に構築できます。

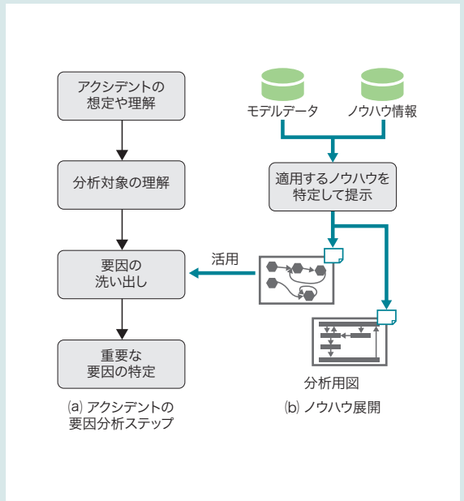

図2．アクシデントの要因分析作業へのノウハウ展開
モデルデータを基に分析対象に応じてノウハウを展開し，要因分析の効率的な実施を支援します。

背　景

DX（デジタルトランスフォーメーション）やSD（ソフトウェアデファインド）化により，複数のシステムが複雑に連携して価値を実現するようになっています。一方で，システムの相互作用が想定外の結果を引き起こすこともあります。特に，アクシデントにつながる要因は，開発の上流で洗い出し，対応策をシステム設計に取り入れることが重要です。ミッションクリティカルな領域を含む場合，発生するアクシデントの要因分析を適切な方法で実施する必要があり，安全分野ではSTAMP/STPA（System-Theoretic Accident Model and Processes/System-Theoretic Process Analysis）や機能共鳴分析（FRAM：Functional Resonance Analysis Method）などの分析手法の適用や応用が試みられています[1], [2]。

また，複雑なシステムの開発技術として，設計対象をモデルで表現し，複数の関係者がシステム全体を捉えながら設計検討を繰り返すMBSEがあります。システムのアクシデントの要因分析は，このMBSEの一環として実施することで設計情報との整合を確保できます。代表的なシステムモデリング言語であるSysML（Systems Modeling Language）の次世代版（v2）では，モデルの意味を表現する構造に従ったテキスト形式で記述することが可能です。これにより，正確な設計情報の共有と各種関連ツールのデータ連携が可能になります。

そこで，SysML v2によるデータ連携を実現するツール環境と，分析手法の実施及びノウハウ活用の仕組みを構築し，システムのアクシデントに関する一層効率的な要因分析を可能にしました。分析に関するノウハウの例には，システムの構成要素に合わせた具体的なガイドワードや，システムの構造に応じた確認内容などがあります。

SysML v2による設計モデルの活用

システム設計のモデリングツールとアクシデントの要因分析で用いるツールの連携はSysML v2のテキスト形式のモデルデータを介して行います（**図1**）。モデリングツールは市販のソフトウェア，分析ツールはオープンソースソフトウェア（OSS）及びフリーソフトウェアを利用しています。モデリングツール上に組み込むSysML v2のモデルデータへの変換機能や，SysML v2のモデルデータから各分析ツール向けの変換機能は自製プログラムで実現しています。モデルデータを扱う標準API（Application Programming Interface）は取り組み時点では開発途上であり，利用していません。

モデリングツールで作成した設計情報のうち，STAMP/STPAやFRAMによる分析で参照する最小限の情報をSysML v2のテキスト形式のモデルデータに変換し，モデルデータ管理環境を介して分析関係者に共有します。分析ツール向けの変換機能がこのモデルデータを参照して各分析用の図の初期案を自動で生成し，以降は分析関係者が編集して分析を実施します。

また，モデルデータ更新時には変更点に基づき分析の再実施が必要となる候補を提示し，各分析で用いる図の初期案も改めて生成します。これにより，再分析の準備の手間を削減し，設計と分析の素早いサイクルを実現します。

アクシデントの要因分析の仕組み

分析では異なる手法であるSTAMP/STPAとFRAMを併用することとし，対象範囲について目安を設けました。STAMP/STPAでは，論理面のアーキテクチャーと物理面のアーキテクチャーを基にシステム内の相互作用によるアクシデント発生の要因を分析します。FRAMでは，主に論理面のアーキテクチャーを基に機能間の処理のループ構造に着目し，正常状態を維持するループ構造を阻害する要因の分析を行います。

アクシデントの要因分析は，四つのステップで行います（**図2**(a)）。要因の洗い出しは，漏れを防ぐために網羅的に実施することが重要であり，ガイドワードを適切に用いる方法も有効です。例えば，制御時間のガイドワードは，長すぎる，短すぎるなどです。対象に合わせて具体的なガイドワードを用いることで，要因の洗い出しの網羅性を高められます。モデルデータを基に分析対象に応じたノウハウを展開する仕組みを構築しており，ガイドワードにもこの仕組みを利用することで，分析関係者が特定する場合に比べて，洗い出せる要因数が最大で10％増加する見込みです。その他の分析ノウハウも，同様の仕組みで分析対象に応じて展開します（図2(b)）。

今後の展望

各関連団体で議論されているSysML v2や，関連ツール，安全分野などにおけるリスク関連データの記述方式の最新動向に対応し，より効果的な仕組みの構築を進めます。また，SysML v2関連で整備が進められている標準APIに対する，評価と適用を検討します。

更に，SysML v2のテキスト形式のモデルデータはLLM（大規模言語モデル）の入力データとして有効と考えられるため，設計とひも付いたアクシデントの要因分析にLLMを活用し，効果向上を図ります。

文　献

(1) Leveson N. G.; Thomas J. P. STPA HANDBOOK. 2018, 188p. <https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf>, (accessed 2024-09-05).
(2) Hollnagel E. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems. 1st ed. CRC Press, 2012, 160p.

羽原　寿和
デジタルイノベーションテクノロジーセンター 先端ソフトウェア技術室
ソフトウェアエンジニアリング技術部