社会情報基盤システムの信頼性保証支援技術

谷津 弘一[†1] 安藤 崇央[†1] 久住 憲嗣[†1] 福田 晃[†1] 孔 維強[†2]

安全・安心な社会情報基盤システムを実現するには，システムの安全性・信頼性を保証する技術が重要となる．我々は，システムのライフサイクルに渡り確立されるトレーサビリティとモデルベースシステム開発技術に着目し，トレーサビリティに基づく不具合の検出技術，並びに，モデルベース開発の上流工程で適用可能な検証技術の研究開発を行っている．本稿では，我々のこれまでの研究成果について紹介する．

Assurance Assistants for Dependability of Social Infrastructure Systems

Hirokazu Yatsu[†1] Takahiro Ando[†1] Kenji Hisazumi[†1] Akira Fukuda[†1] and Weiqiang Kong[†2]

To develop dependable social infrastructure systems, technologies to assure their dependability would be essential. The authors consider traceability established through system life cycle and model-based system engineering are important for such technologies. This paper introduces a method to detect vulnerable points of systems based on traceability and a model checker applicable to SysML diagrams, both of which the authors have been developing.

1. はじめに

人々の生活を支える社会情報基盤システムにとって，安全かつ安心なものであることは，必ず達成されなければならない最も基本的な要件である．それ故に，システムの信頼性（本稿では，以降，システムの安全性や安心性を含めて，信頼性と呼ぶことにする）を保証する技術は，社会情報基盤システムの開発・保守において重要な技術であると言える．

我々は，システムのライフサイクルの中で作り出される様々な資料の間に確立されるトレーサビリティに基づき，システムの信頼性の保証 – より詳しく言えば，システムがその安全性や安心性を損なう状況に陥るリスクが許容範囲内に収まっていることの保証 – を支援する仕組みの研究開発を行っている．

本稿では，安全・安心な社会情報基盤システムの開発技術に関する議論の材料として，現在我々が開発している技術のうち，次の2つを紹介する．1つは，システムの中で，信頼性を損なう危険のある脆弱な箇所を，システムの開発の上流工程で作成される以下の 3 種類の資料の間に確立されるトレーサビリティに基づき検出する仕組みである．

- システムの安全性・安心性を損なう状況を引き起こす障害事象
- 障害事象が発生するリスクを許容範囲内に軽減するために達成されるべきゴール
- システムの設計資料

そして，もう一つは，SysML 図に適用可能なモデル検査器である．システム開発のコストを考えれば，設計段階である程度の形式検証を行えるようにしておくことが望ましい．設計段階で形式検証を行うことができれば，設計が与えられた要求や制約を満足することを示す質の高い証拠を提示することができる．これは，システムの信頼性の保証に寄与する．我々は，近年その重要性が認識されているモデルベース開発技術，その中でも，開発の上流工程から適用できる SysML[1]に着目し，SysML で記述されたブロック図，ステートマシン図，パラメトリック図等の上でモデル検査ができるような仕組みの研究開発も行っている．

†1 九州大学
Kyushu University
†2 大連理工大学
Dalian University of Technology

2. 開発中の信頼性保証支援技術

2.1. 信頼性脆弱箇所の検出

信頼性を損なう危険のある脆弱な箇所の検出は，前節で挙げた，障害事象，ゴール，設計資料の間に確立されるトレーサビリティ（図 1）に基いて行われる．

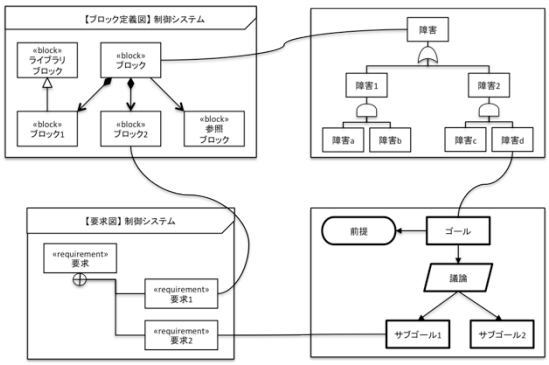

図 1 脆弱箇所検出に用いられるトレーサビリティ

Fig.1 Traceability used in detection of vulnerable points

上図の左側は，SysML で記述されたブロック図と要求図である．このトレーサビリティが確立される設計情報は，モデル検査器の場合と同様，SysML 図を想定している．そして右上は FTA や FMEA 等の分析手法に基づき洗い出される障害事象の因果関係であり，右下は障害事象発生の否定をゴールとする保証ケースである．この保証ケースの葉となるサブゴールが，障害事象が発生するリスクを許容範囲内に軽減するために達成されるべきゴールを表す．トレーサビリティは，次の要素間で確立される．

1. SysML ブロックと障害事象
2. 障害事象とゴール
3. (サブ)ゴールと SysML 要求
4. SysML 要求と SysML ブロック

1.は，ブロックに障害事象が発生すること，2.は，ゴールが障害事象の発生の否定であること，3.は要求が満たされればゴールが達成されること，4.は，ブロックが要求を満たすことを，各々表している．ブロックに障害事象が発生しないことを言うためには，その障害事象を発生させないために必要なゴールが達成されていることを示せば良い．これは，ゴールの達成を保証する要求とブロックの間にトレーサビリティが確立されていることで導かれる．システムの信頼性税泊箇所の検出は，洗い出された障害事象が発生しうるブロックを洗い出すことで行われる．

2.2. SysML 図上でのモデル検査器

我々が開発している SysML 図上でのモデル検査器[2]は，正確に言うと，既存のモデル検査器や SMT ソルバへのインターフェースである．今のところ，既存のモデル検査器として PAT[3]を採用している．

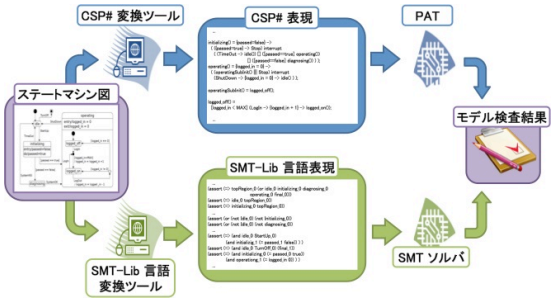

図 2 SysML 図上でのモデル検査器

Fig.2 Our model checker on SysML state machine diagrams

このインターフェースは，指定に応じて，与えられた SysML ステートマシン図をモデル検査器 PAT への入力言語である CSP#[3]や SMT ソルバへの標準入出力言語である SMT-Lib 言語による表現に変換する．一般に， PAT や SMT ソルバへの入力を生成するには，ステートマシン図だけでは情報が不十分なので，必要に応じて，ブロック図，シーケンス図，パラメトリック図等から情報を補っている．

3. まとめ

現在，我々が開発している技術のうち，システムの信頼性脆弱箇所検出の仕組みと SysML 図上でのも出る検査器を紹介した．本ワークショップでは，これらを材料として，安全かつ安心な社会情報基盤システムをどのように開発すべきかについて議論したい．

参考文献

[1] OMG, “OMG System Modeling Language Version 1.3”, available at http://www.omg.org/spec/SysML/1.3/PDF, 2012.

[2] Takahiro Ando, et.al., Formalization and Model Checking for SysML State Machine Diagrams by CSP#, Proc. Int. Conf. on Computational Science and Its Applications (ICCSA 2013), pp.114-127, Springer, 2013.

[3] J.Sun, Y.Liu, J.S.Dong, Model Checking CSP Revisited: Introducing a Process Analysis Toolkit, Proc. Int. Symp. on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2008), pp.307–322, Springer, 2008.