15-B-1

SysML と CML によるシステムオブシステムズの検証 [1]

1. 適用した技術や手法の概要

システムオブシステムズ（SoS：System of Systems）は複数のシステムから構成され機能するシステムである。構成要素である各システムは独立した異なるシステムであり、個別に管理・運用される。そのため、各構成システムをシステムオブシステムズとして開発・運用することは困難であると言われている。

ここでは、SOS 緊急応答システムに SysML[2] と CML[3] を適用し、モデリングツールを利用しながら統合開発環境で形式検証を行った事例を紹介する。

1.1. 背景

イタリアのソフトウェア開発企業である INSIEL 社 [4] は、緊急応答ユニットのシステム、消防隊のシステム、山岳救助隊のシステム、電話システム、無線通信網、電話通信網などの複数のシステムを管理する統合緊急コールセンター（CUS：Centrale Unica di Soccorso）のシステムを開発し、運用している。ここで、統合緊急コールセンターのシステムを含む各構成システムからなるシステム全体を SOS 緊急応答システム（図 15-B-1-1）と呼ぶ。

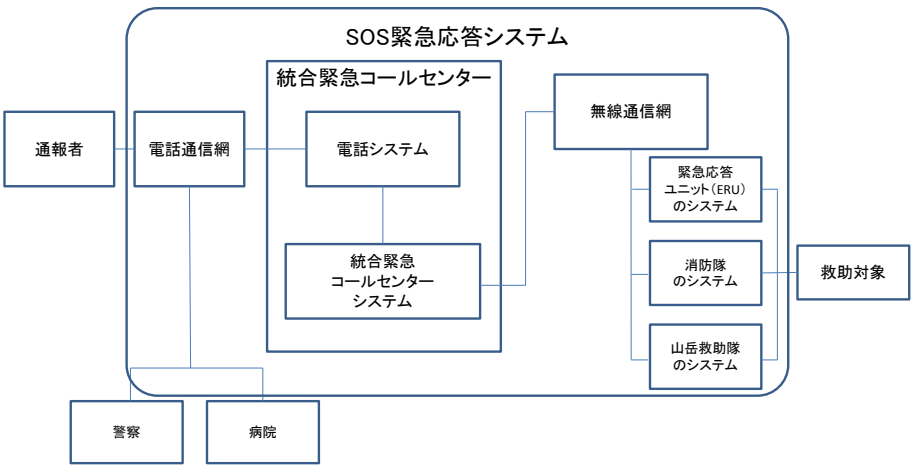

図 15-B-1-1　SOS 緊急応答システム

[1] 事例提供: Newcastle University　Centre for Software Reliability School of Computing Science John Fitzgerald 氏

[2] Systems Modeling Language

[3] Compass Modelling Language

[4] INSIEL 社はソフトウェアシステムの開発、インテグレーションのサービスを提供するイタリアの企業。民間企業ではあるが、地方政府、市の機関、健保医療機関により 100%所有されている。

図 15-B-1-1 の角の丸い枠内が統合緊急コールセンターのオペレータが直接管理するシステムであり、警察システムや病院システムは、直接管理しないので SOS 緊急応答システムの枠外に位置付けた。

統合緊急コールセンターは、各構成システムのリソース（人員や機材など）の状況をオンタイムで把握しつつ、緊急時には一体化したシステムとして振る舞う必要がある。ユーザーからの緊急コールを受けると、統合緊急コールセンターは、その内容を把握するとともに、緊急応答ユニット、消防隊、山岳救助隊などとシステム的に連携し迅速な対応を促す役割を果たしている。

1.2. 課題

SOS 緊急応答システムの各構成システムは複数の異なる関係者により独自に開発されており、仕様の記述方法や記述のレベルは異なっている。このため、以下の問題があった。

- SOS 緊急応答システム全体を仕様として把握し形式検証することが困難
- SOS 緊急応答システムの構成システムに仕様変更が生じた場合、変更のトラッキングおよび形式検証することが難しい
- SOS 緊急応答システムに構成システムが追加される場合、その把握および形式検証が困難

この結果、SOS 緊急応答システムの仕様書は曖昧なままであり、それに基づいて開発された構成システムと SOS 緊急応答システムの検証は不十分であり、信頼性についても不安があった。

1.3. 手法の概要

各構成システムにモデリングツール（Atego 社の Artisan：「5.開発体制や開発ソフトウェア等の確認」参照）を使用しシステム記述言語である SysML で記述した。SysML はシステムを記述できるが、形式検証はできないため、形式言語である CML（Compass Modelling Language）[5]に変換した。CML は、形式言語である VDM[6]（データと機能モデルを記述）や CSP[7]（プロセス計算を記述）を組み合わせた形式言語であり、CML に変換したシステム記述は統合開発環境（Symphony：「5.開発体制や開発ソフトウェア等の確認」参照）を使い形式検証ができるようになった。

---

[5] SysML で定義された SoS のモデルを形式検証可能なモデルにする形式記述言語

[6] 形式手法の 1 つであり、1960 年代に IBM ウィーン研究所で開発された
VDM information Web site：http://www.vdmtools.jp/

[7] Communicating Sequential Processes　Oxford 大学の Tony Hoare が 1979 年に考案したもので、並列処理で必要とされる基本的な動作を記述するプロセス代数
CSP コンソーシアムの Web site：http://www.csp-consortium.org/csp/

2. 適用した技術や手法の導入に踏み切った理由や経緯

INSIEL 社は、1.2 で示した課題を解決するために、SOS 緊急応答システム全体を SysML で記述して形式検証ができる方法を探していた。このとき、欧州の開発フレームワーク（FP7[8]）のプロジェクトである COMPASS[9] ではシステムオブシステムズの仕様記述方法および検証方法が検討されていた。そこで INSIEL 社は、COMPASS の研究テーマの 1 つである CML とツール（「5.開発体制や開発ソフトウェア等の確認」参照）に着目した。

CML は、システムオブシステムズの形式検証が可能であるため、SOS 緊急応答システムに応用できると考えた。そこで、INISIEL 社は COMPASS プロジェクトに参画し、システムオブシステムズのアプローチでシステム全体をモデル化し検証する技術を習得、蓄積することで将来的にメリットがあると考えた。

3. 適用のための事前準備や工夫

UML での開発経験がある開発者が SOS 緊急応答システムの SysML によるモデル化を担当した。このため比較的短期間にモデル化を進めることができた。CML については、積極的に COMPASS プロジェクトの活動に参加することで、技術の習得を図った。

ただ、INSIEL 社の開発者にとっては、SysML や CML は馴染みのない言語であったため、本手法を利用するには SysML 、CML の理解、および Symphony を含む各種のツールを使いこなすためにかなりのトレーニングが必要になった。

また、前述の課題に対応するために以下の準備を行った。

（1） SOS 緊急応答システムの視覚化の準備

SOS 緊急応答システムの仕様を SysML で記述し視覚化する準備として、INSIEL 社は構成システムの仕様書やマニュアルを取り揃え整理した。また、緊急コールを受信し、緊急事態の状況、リソース（人材、車両、機器等）を把握し対応する応答シナリオを事前準備した。

（2） 構成システムの更新に向けた準備

通常、構成システムは継続的に更新されるため、INSIEL 社が変更を管理しトラッキングすることは難しい。構成システムの仕様に変更があった場合にその変更内容を入手できるように、構成システムを開発する組織やプロバイダにプロジェクトの目的と効果を事前に説明した。

（3） 新しい構成システムの追加の準備

現状の構成システムに新たな構成システムが加わった場合に起こる影響を、モバイル電話のシステムで事前に分析した。

---

[8] Seventh Framework Programme for Research：欧州委員会の 2007 年～2013 年にわたる第七次研究枠組み計画

[9] http://www.compass-research.eu/index.html

4. 適用した技術や手法の効果測定の方法とその結果

SOS 緊急応答システムを SysML と CML でモデル化することにより、その仕様を視覚化し、確認・形式検証することができた。また、緊急コールを受けてから、統合緊急コールセンターが指令を発するまでの一連の手順を視覚化するとともに検証することができた。

この結果、統合緊急コールセンターおよび SOS 緊急応答システム全体の信頼性が向上した。特に下記の効果があった。

（1）　SOS 緊急応答システムの視覚化とシステム品質

SOS 緊急応答システム全体を SysML で記述することで、モデリングツールである Atego 社の Artisan Studio（「5.開発体制や開発ソフトウェア等の確認」参照）を使いシステム全体の仕様を視覚化した。これにより、SOS 緊急応答システム全体の仕様を把握することができた。

図 15-B-1-2 に統合緊急コールセンターと他の構成システムの入力と出力の関係を視覚化（インターフェースの視覚化）した例を示す。図 15-B-1-2 では、半円は情報の受け口を表し、青の〇は情報の出口を表している。

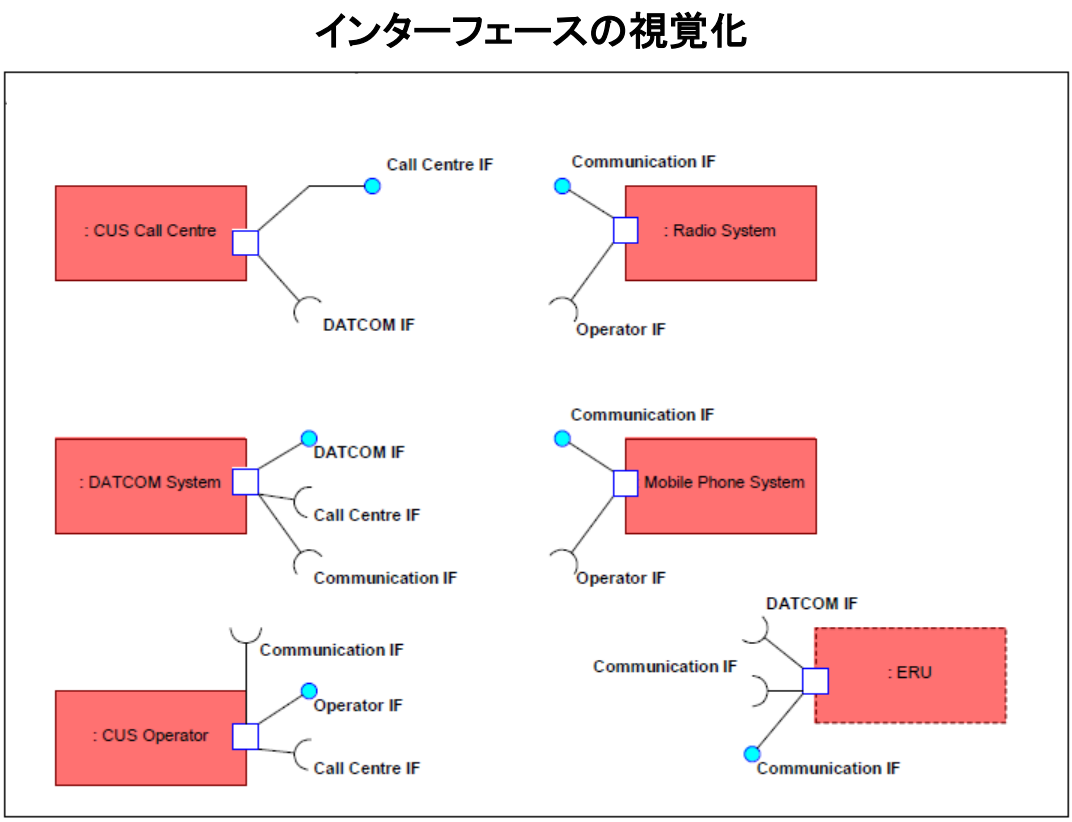

図 15-B-1-2　SOS 緊急応答システムの視覚化（インターフェースの視覚化）の例

図 15-B-1-3 に緊急コールを受信し処理する手順を視覚化（応答シナリオの視覚化）した例を示す。

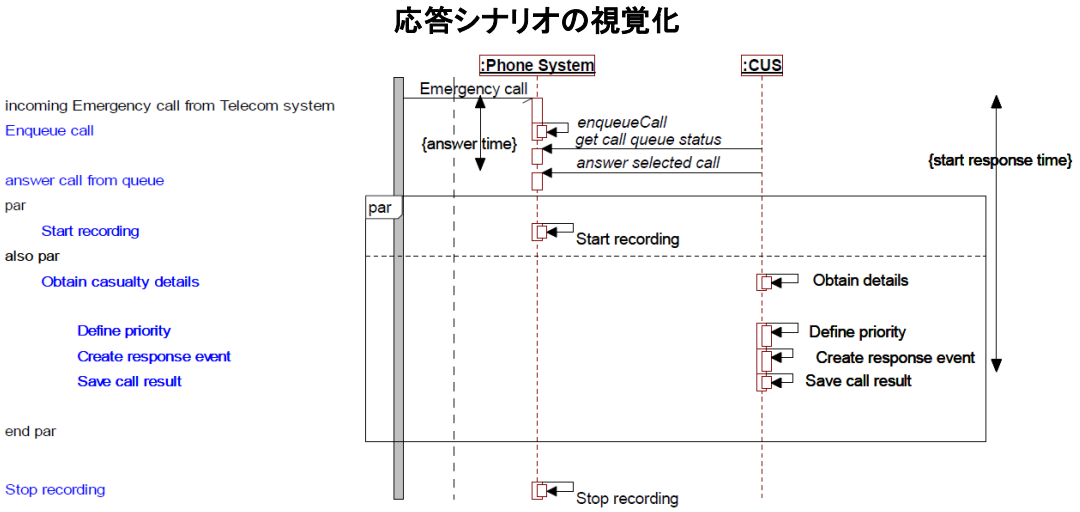

図 15-B-1-3　SOS 緊急応答システムの視覚化（応答シナリオの視覚化）の例

また、SysML のモデルを CML に変換し、Symphony 統合開発環境（「5.開発体制や開発ソフトウェア等の確認」項参照）を使用して形式検証を行った。

SysML でシステムの仕様を視覚的に確認し、CML で形式検証することで、SOS 緊急応答システムの障害や不具合を早期に検出できた。これにより SOS 緊急応答システムの品質が向上した。

（2）　SOS 緊急応答システム全体で起こる変更の影響の把握

SOS 緊急応答システムを構成する緊急応答ユニットのシステム、消防隊のシステム、山岳救助隊のシステム、電話システム、無線通信網、電話通信網システムは、変更や再構成を繰り返しながら進化していく。INSIEL 社では、このような構成システムの進化が SOS 緊急応答システムや各構成システムにもたらす影響を分析すること（例：要件の変更により影響を受ける構成システムをトレースできる等）ができるようになった。SOS 緊急応答システムの構成システムに仕様変更が生じた場合でも、変更のトラッキングおよび形式検証をすることが可能になった。

（3）　構成システムの追加

構成システム追加による影響を分析するとともに、起こり得るリスクを特定し、プロアクティブな対応をすることができた。図 15-B-1-4 は構成システムにモバイル電話システムが追加された例を示す（赤太線で表記）。この追加により SOS 緊急応答システム全体や他の構成システムに及ぼす影響を分析できた。SOS 緊急応答システム全体、構成システムが追加される場合、その把握および形式検証ができるようになった。

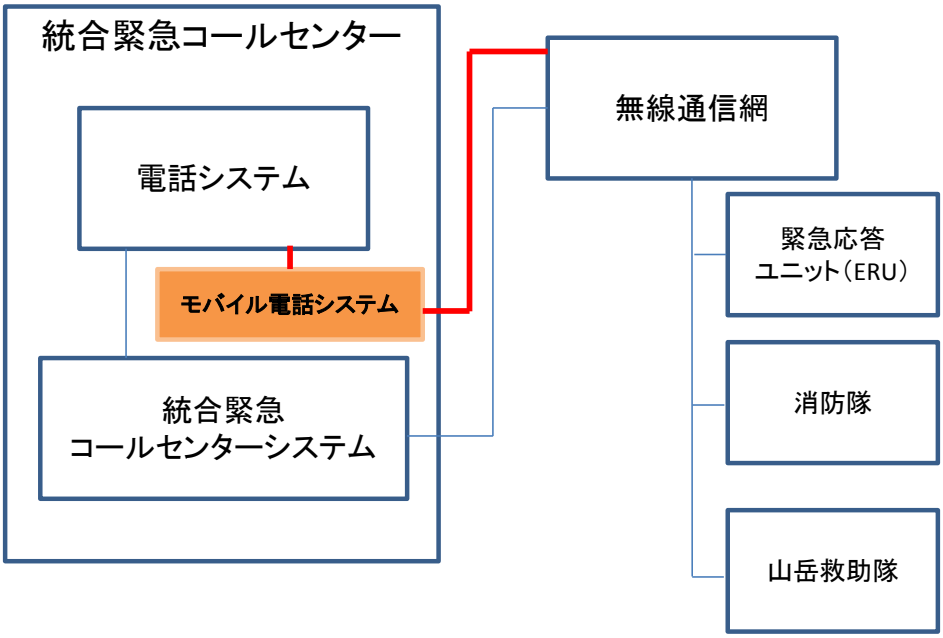

図 15-B-1-4　モバイル電話システム（構成システム）の追加

5. 開発体制や開発ソフトウェア等の確認

INSIEL 社は EU の研究開発フレームワーク（FP7）のプロジェクトの 1 つである COMPASS の成果を活用することとした。

図 15-B-1-5 に INISIEL 社が本プロジェクトで使ったツールの関連図を示す。

SOS 緊急応答システムの検証では、これらのツールを次の手順で利用した。

- Atego[10] 社の Artisan Studio を使用し、SysML で SOS 緊急応答システムのモデルを作成した。
- このモデルを使い、Artisan Studio の機能で SOS 緊急応答システムの仕様を理解しやすいグラフィカルな複数のビューで確認した。
- 外部接続された HiP-HOPS ツールで SysML モデル記述された SOS 緊急応答システムのフォールトトレラント分析を行った。
- SOS 緊急応答システムの SysML モデルを CML モデルに変換した。
- CML で記述された SOS 緊急応答システムを COMPASS プロジェクトで開発された、Symphony と呼ばれる各種ツールの統合開発環境（IDE）を使用し分析した。

Symphony 統合開発環境は自動定理証明ツール（Isabelle）やモデルチェッカー（Microsoft FORMULA）、モデルテストツール（RT Tester）などの分析ツールをプラグインできる。これらの分析ツールにより、SOS 緊急応答システムの仕様を形式検証することができた。

---

10 モデルベースのシステムおよびソフトウェアエンジニアリングアプリケーションの開発企業、2014 年 6 月に PTC 社により買収された。PTC 社の Web サイト：http://ja.ptc.com/about/history/atego

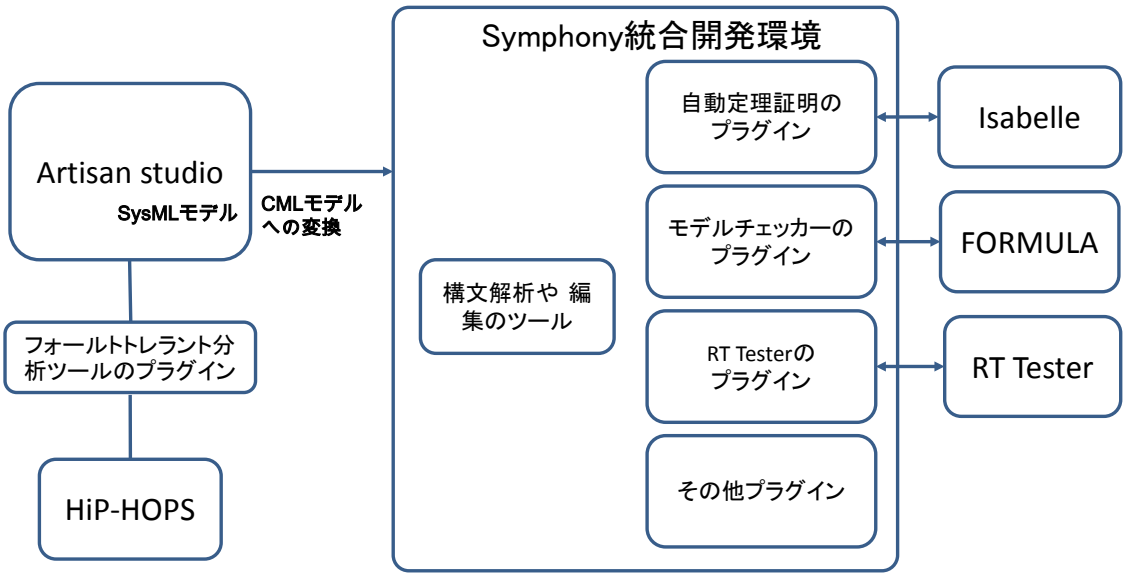

図 15-B-1-5　使用したツールの関連図

以下はプラグインされたツールである。それぞれを説明する URL を参考文献に示す。

- HiP-HOPS ツール：Hull 大学で開発されたフォールトトレランス分析ツール[7]
- RT-Tester：自動テスト生成、テスト実行、リアルタイムテスト評価を行うテスト自動化ツール[8]
- Isabelle：形式言語で表現された記述の証明を行う自動定理証明ツール[9]
- Microsoft FORMULA：Microsoft Research が提供するモデルチェッカー[10]

6. 適用結果と今後の取組み

6.1. 品質について

SysML と CML を使い、SOS 緊急応答システムをモデル化することで、構成システム間の連携の問題を早期に発見し解決できる。また、構成システムの変更や追加・統合によって生じる問題も早期に抽出できる。

SOS 緊急応答システムの変更が及ぼす影響や意味について、モデルなしに理解するのは難しい。構成システム相互の関係が明確に定義されていないと、SOS 緊急応答システム全体に予期しない不具合を引き起こす可能性がある。

INSIEL 社は、SysML と CML のモデル化により、SOS 緊急応答システムで起こる仕様変更の影響を把握することで、不具合の発生を予測し品質が向上することが可能となった。

6.2. 生産性について

SysML と CML によって記述された SOS 緊急応答システムのモデルは、複数の開発者が共有できるドキュメントの役割を果たす。また、共有された情報を構成システムなどにフィードバックすることができる。したがって、SOS 緊急応答システムのシステム全体で正確に

要件定義ができるため、不具合や手戻り作業が減少する。このため、生産性が向上する。

6.3. 検証への影響

SysML と CML によって SOS 緊急応答システムを記述することで、システム全体の振舞いから構成システムの仕様を検証することができる。また、統合緊急コールセンターの応答シナリオを事前に分析し、統合緊急コールセンターのシステムの仕様に反映することができる。この結果、統合緊急コールセンターシステム機能の妥当性検証を実環境で実施する工程を大幅に短縮することができた。

6.4. 今後の取り組み

INSIEL 社では、SysML や CML、その関連ツールや手法を導入し、成果が得られたことから、今後は社内で専門用語や手法の共有化を図るとともに、開発要員の知識レベルと技術レベルを引き上げる予定である。特に、SysML や CML をモデルベース開発における社内の標準技術にしていく予定である。

また、今後、SOS 緊急応答システムに森林警備隊のシステムや防災部門のシステムを追加することが考えられる。また、システムオブシステムズの新規開発も含め、金融など他の領域のプロジェクトにも適用する予定である。

7. まとめ

複数のシステムからなる SOS 緊急応答システムをシステムオブシステムズとして、SysML や CML でモデル化した。これにより、SOS 緊急応答システムの仕様を視覚的に把握すると同時に形式検証が可能になった。緊急要請の業務手順のシミュレーション、フォールトトレランス分析を実施することが可能となり、システム更新や機能追加時の影響を把握できるようになった。

従来の独立的で自律的なシステムであってもシステムオブシステムズとしてシステム間の相互連携が必要な場合が増えている。例えば、公共サービスでは、複数の公共機関が協調してサービスを提供するためにシステムの連携が求められる。このように、複数システムの連携する「つながるシステム」が増えることで、システムオブシステムズの信頼性、安全性を維持する技術や手法はますます重要になると考えられる。

参考文献

[1] COMPASS, Accident Response Use Case Engineering Analysis Report Using COMPASS Methods & Tools, Document Number：D41.2, 2014
http://www.compass-research.eu/Project/Deliverables/D41.2.pdf
[2] COMPASS, Accident Response Use Case Engineering Analysis Report Using Current Methods & Tools, Document Number：D41.1, 2013
http://www.compass-research.eu/Project/Deliverables/D411.pdf
[3] COMPASS, Report on Guidelines for System Integration for SoS, Document Number：D21.4, 2013
http://www.compass-research.eu/Project/Deliverables/D214.pdf
[4] Claire Ingram, Steve Riddle, John Fitzgerald, Sakina A.H.J. Al-Lawati, Afra Alrbaiyan：SoS Fault Modelling at the Architectural Level in an Emergency Response Case Study　http://arxiv.org/pdf/1404.7778.pdf
[5] Zoe Andrews, John Fitzgerald：COMPASS:Advanced methods and tools for model-based systems-of-systems engineering, 2014
http://www.incoseonline.org.uk/Documents/research/COMPASS_ASEC2014_Zoe_Andrews.pdf
[6] COMPREHENSIVE MODELLING FOR ADVANCED SYSTEMS OF SYSTEMS
http://www.atego.com/downloads/support/docs/COMPASS.pdf
[7] HiP-HOPS ツール Hull 大学で開発されたフォールトトレランス分析ツール
http://www2.hull.ac.uk/science/computer_science/news_and_events/news/hip-hops_goes_commercial.aspx
[8] RT-Tester 自動テスト生成、テスト実行、リアルタイムテスト評価を行うテスト自動化ツール https://www.verified.de/products/rt-tester/
[9] Isabelle 形式言語で表現された記述の証明を行う自動定理証明ツール
http://isabelle.in.tum.de/overview.html
[10] Microsoft FORMULA, Microsoft Research が提供するモデルチェッカー
http://research.microsoft.com/en-us/projects/formula/default.aspx