Research Center for Verification and Semantics
産業技術総合研究所 システム検証研究センター
News Letter
10
2008.09

形式手法≠モデル検査

CVS 発足の 2004 年には、形式手法はまだ、特別な技術としてみられがちで、とくに組込ソフトウェア技術者にはほとんどしられていなかった。しかし、組込ソフトウェアが急激に大規模になったために、形式手法が注目されるようになった。機能安全の自動車分野向け規格 ISO26262 の策定活動がはじまり、車載ソフトウェアの安全性とそれを支える信頼性が問題になっていることも、これに拍車をかけているかもしれない。

これと相前後して、ソフトウェア工学研究者の間で、形式手法による検証法の一つであるモデル検査がつかわれはじめた。モデル検査は 1970 年代後半に基礎理論がだされ、90 年代後半にはすでにハードウェアの検証の一手法としてもちいられていたが、2000 年前後からソフトウェアへの応用がはじまった。

このように、わが国の組込ソフトウェアの世界では、形式手法とモデル検査が同時期に導入されることになった。そのためか、形式手法＝モデル検査、あるいはそこまでいかなくとも、形式手法＝形式的検査手法、という誤解がみられる。しかし、形式手法は検証のみならず、システム開発過程全般の手法とみるのが適当であろう。実際、1980 年代に形式手法が我が国のソフトウェア工学界に導入されたときには、仕様記述、つまり設計の技術としての側面が強調されたものである。

もともと設計工程が完全なものであれば、検証は不要な筈である。もちろん完全な作業工程などというものはあり得ないので、検証が不要になることはなかろうが、設計工程がもっと当てになるものにするような考察も大切であろう。形式手法研究のなかにも設計工程に影響をあたえる考察がたくさんある。

すると、形式手法というのは一体何なのだ、検査法だったり設計法だったり、ヌエの如きものではないか、という声がきこえてきそうである。全くその通りで、実は「形式手法」という一つの方法が提案されているわけではない。筆者は形式手法というのは数理科学的な裏付けをもったプログラミングの研究全般、あるいはその応用部分をさしているのだとかんがえている。だとすると、多様な応用の局面があっても不思議はないのだ。

2008 年 9 月
システム検証研究センター
研究センター長 木下 佳樹

＜ＣＶＳニュースレター 10 号＞

産業技術総合研究所 システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト ：〒 560-0083 大阪府豊中市新千里西町 1-2-14 三井住友海上千里ビル 5F
●関西センター：〒 563-8577 大阪府池田市緑丘 1-8-31

●トピックス１

2007 年度 システム検証研究センター 研究プロジェクト報告会

昨年度に引き続き、2007 年度に CVS/AIST において実施された各研究プロジェクトの報告会を開催いたしました。CVS/AIST の一年間の研究活動内容全体の総括を行なうとともに、実施したプロジェクト毎に担当研究者による、より詳しい発表も行ないました。

開催日：2008 年 3 月 13 日（木）
場　所：産業技術総合研究所関西センター
融合棟２F 多目的ホール（大阪府池田市緑丘 1-8-31）

本レターでは、全プロジェクトの研究発表概要をご紹介させていただきます。発表内容はテクニカルレポートにまとめて冊子として発行しておりますので、ご希望の方は、当センターホームページよりお申込ください。また、ホームページより直接ダウンロードも可能です。

http://unit.aist.go.jp/cvs/techrep.html

2007 年度システム検証研究センター 研究プロジェクト報告会 全１３研究発表概要

1. CREST 研究総括

五年計画の最終年度。本計画で開発したポインタ処理プログラムを対象とする最弱事前条件計算器 pfvalid と定理証明支援系 Agda を本計画で提案する Agda-IVE の枠組で連携させて用い、実在のソフトウェア YAMPII の待ち行列処理システムの信頼性を評価する実験を行って、Agda-IVE のフィージビリティを検討した。その結果、繰り返し文における不変条件を確定することをはじめとする、検証項目論理式の確定の段階に、Agda と pfvalid の Agda-IVE による連携が極めて効果的に作用することを確認した。

2. 数理モデル研究

班長：木下佳樹
班員：岡本圭史、高井利憲、竹内　泉、山形頼之

プログラミング意味論の研究を行うことを目的としている。我々が提案した一階様相 μ 計算の恒真命題は帰納的に枚挙不能であり、従って完全性が成立し得ないことは二年前に明らかにしていたが、高階論理の場合と同様にして、一般完全性の概念を導入して、一回様相 μ 計算が一般完全であることを示した。その他、PML の意味論を不動点付様相論理の代数的意味論の一般論を用いて与える試みも行った。

3. 抽象化ツール研究開発

班長：高橋孝一
班員：関澤俊弦、田辺良則、湯浅能史

ポインタを操作するプログラムのソースコードを網羅的に検証するためには、抽象化が必須である。我々は、ポインタ操作をするソースコードから、抽象化された状態遷移系を自動生成する MLAT ツールを改良し、高度なプログラムの検証を可能にした。

4. 対話型検証研究

班長：加藤紀夫
班員：齋藤正也

対話型証明支援系 Agda と Agda から外部の自動検証器を呼び出す機構を組み合わせることにより、統合検証環境 Agda-IVE を開発した。また実際に Agda-IVE を使って MPI 通信ライブラリ YAMPII のポインタ操作の検証を行い、対話型検証と自動検証の両方を扱える環境の有用性を実証した。

5. フィールドワーク１

班長：高井利憲
班員：大崎人士、尾崎弘幸、吉田　聡、中野昌弘 、（竹内　泉）

矢崎総業と共同研究で、数理的技法をソフトウェアの開発現場に導入するための研究を行い、本年度は、昨年度までの成果をまとめることを中心に以下の成果を得た。組込みソフトウェアの効率的なモデル化技術である環境ドライバや検査式の図的で直感的な表現である図示記法、n 点通過テストのための検査手法を提案した。また、いくつかのモデル検査実験も手がけた。

6. フィールドワーク２

班長：高橋孝一
班員：竹内　泉、高木　理

業務フロー図の作成を支援し、検証を行なうシステム AWV を開発した。この AWV の製作に際して開発された業務フロー図を検証する技術を特許として出願した。

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

7. フィールドワーク４

班長：湯浅能史
班員：水口大知、渡邊　宏

自動車関連企業と共同で、対話的証明支援系を用いた車載ソフトウェアの検証について事例研究を行った。実験用に策定された電子制御ユニットのデータフロー図仕様を Agda 言語で記述した。更に調停器と呼ばれるユニットに関して、その基本性質を演繹的な証明によって検証した。

8. フィールドワーク６

班長：高井利憲
班員：吉田　聡

共同研究により、アセンブラで記述された組込みシステムに対して数理的技法による不具合解析を試みた。結果として、不具合の全容解明には至らなかったが、新たなソースコード上の脆弱性を発見した。また、ソースコードからの半自動的なモデリングや、不具合現象の原因候補の選別のための手法（不具合の原因にならないこと示すために行った足踏同値なモデルの作成）が得られた。

9. フィールドワーク７

班長：岡本圭史
班員：安部達也、齋藤正也、武山　誠

従来人手により行われていたシステム LSI 用検証項目の生成作業を自動化する為に、Agda 言語を用いて、仕様書の一部形式化と検証項目生成器の試作を行った。なお、本研究は株式会社ルネサステクノロジとの共同研究であり、JST からの受託研究の一環として行われた。

10. 研修コース開発

班長：西原秀明
班員：木下佳樹、高木　理、高村博紀、中原早生
渡邊　宏、岡本圭史、高橋孝一

「モデル検査研修コース中級編 / 上級編」の開発を行った。中級編について 18 年度の成果としてつくられていた教材を文書化してまとめた。上級編については教材作成を行い、ドラフト版を完成させた。数理的技法の教育について議論するワークショップを四回開催した。このワークショップを発端に、数理的技法の新たな教育プログラムを共同で開発する活動も始まっている。

11. ソフトウェア認証研究

班長：水口大知
班員：長谷部浩二

主には「機能安全対応自動車制御用プラットフォームの開発」において活動したが、加えて、ソフトウェアにおける機能安全についての解説記事の執筆も行った（信頼性学会誌）。また、産総研計測標準研究部門と共同で、計量器の遠隔校正システムの妥当性確認を ISO/IEC 17025 に沿って行うための研究を開始した。

12. 知識様相論

班長：竹内　泉
班員：矢田部俊介

知識様相論理研究班は、証明支援系 Agda 上で、知識様相論理の意味論（充足関数）の実装をおこなった。この様相論理は、不確かな、誤りを含む情報から正しい結論を導出することを目的とした体系であり、ネットワーク上の個人認証技術などへの応用が期待される。

13. 事例報告データベース

班長：渡邊　宏
班員：奥野康二、高井利憲

H14 年度以後にシステム検証研究センターあるいはその前身であるシステム検証研究ラボで実施した、システム検証の科学技術に関する事例研究について、それを詳しく説明する論文、テクニカルレポートなどの情報への参照を収集した。

まとめた「システム検証の事例報告集 2007 年度版」をテクニカルレポートとして出版するとともに、Web 版をユニットの公式ホームページ上でも公開した。

http://unit.aist.go.jp/cvs/jireihoukoku/index.html

プロジェクト報告会開催風景

シンポジウム開催のお知らせ

第五回システム検証の科学技術シンポジウム

The 5th Symposium on System Verification (SSV 2008)

日程：2008 年 11 月 17 日 (月) ～ 11 月 19 日 (水)
場所：筑波大学大学会館 国際会議室 (つくばキャンパス)
主催：日本ソフトウェア科学会ディペンダブルシステム研究会
共催：産業技術総合研究所 システム検証研究センター
筑波大学大学院 システム情報工学研究科

詳細はこちらをご覧ください。▼
http://unit.aist.go.jp/cvs/symposium/sympo-top.html

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●トピックス２

プレスリリース

平成 20 年 5 月 23 日

ソフトウェア信頼性技術の研究開発・人材養成の産学官連携活動を強化
―ソフトウェア信頼性技術の中核施設―

独立行政法人 産業技術総合研究所【理事長 吉川 弘之】（以下「産総研」という）は、関西センターにおいてソフトウェア信頼性技術の中核施設を整備して、先端研究、技術移転および技術者養成活動を加速することとした。

近年、組込みシステムの需要が急拡大したため、その不具合が発生すると影響が大きく、信頼性向上が重要かつ緊急の課題である。産総研では、関西センターに設置したシステム検証研究センターにおいて数理的技法（形式手法）を中心にシステム検証技術の研究活動を展開してきたが、更にその活動を広げるためにこの中核施設を整備することとなった。

具体的には、組込みシステム検証試験施設を設け、利用を産業界および学界に開放して、検証技術の先端研究、技術移転の産官学連携活動を開始する。また、組込みソフト産業推進会議【会長 宮原 秀夫】と共同で組込みシステム高度技術者養成のための「組込み適塾」【塾長 今瀬 真】を開講し、日本全国で 10 万名不足していると言われる組込みソフトウェア技術者の養成に取り組む。

http://www.aist.go.jp/aist_j/press_release/pr2008/pr20080523/pr20080523.html

平成 20 年 7 月 22 日

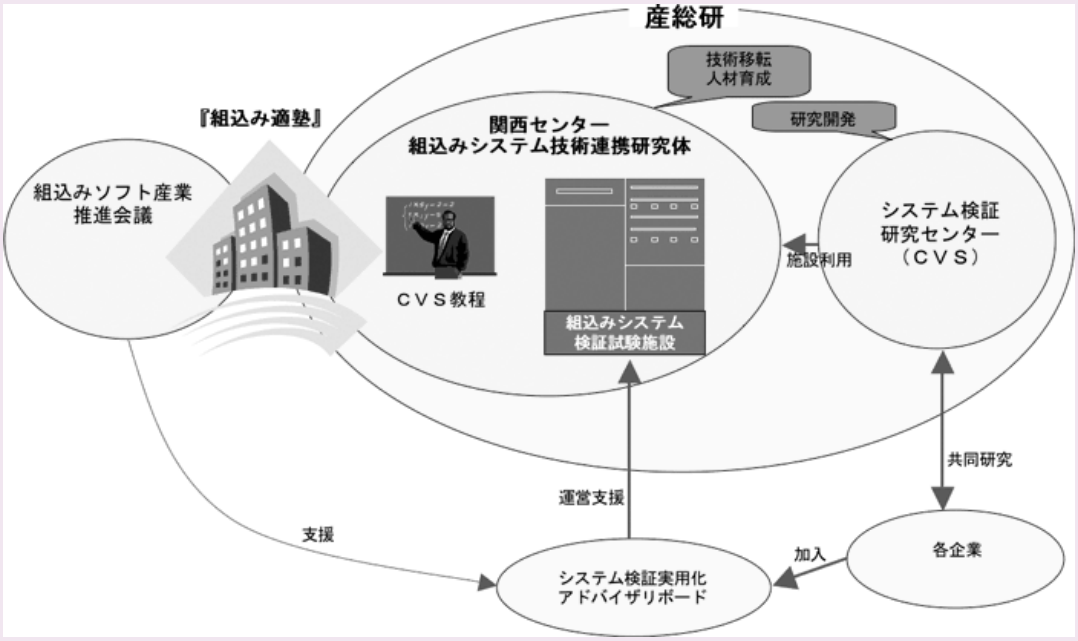
高度組込みソフトウェア技術者養成のための「組込み適塾」を開塾
― 組込みシステム検証試験施設を用いた技術移転と人材養成を担う組織も発足 ―

独立行政法人 産業技術総合研究所【理事長 吉川 弘之】（以下「産総研」という）は、組込みソフト産業推進会議【会長 宮原 秀夫】と共同で、高度組込みソフトウェア開発技術者を養成する「組込み適塾」【塾長 今瀬 真】を 7 月 22 日に開塾した。

また、関西センターにおいて、7 月 1 日に、新たに「組込みシステム技術連携研究体」【連携研究体長 神本 正行】を発足させ、組込みシステム検証試験施設を用いた最先端検証技術に関する技術移転と人材養成事業を推進する体制を固め、「組込み適塾」の運営を実施していく。

近年、組込みシステムの需要が急拡大したため、その不具合が発生すると社会的影響が大きく、信頼性向上が重要かつ緊急の課題である。産総研では、関西センターに設置したシステム検証研究センター【研究センター長 木下 佳樹】において数理的技法（形式手法）を中心にシステム検証技術の研究活動を展開してきたが、さらにその活動を広げるためにこの中核施設を整備する。組込みシステム検証試験施設を整備するとともに、技術移転と人材養成事業を推進して組込みシステム技術者の全国的な不足に対応し、組込みシステムの信頼性確保に貢献する。

http://www.aist.go.jp/aist_j/press_release/pr2008/pr20080722/pr20080722.html



産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

● CVS ニュース

AIM8 活動報告

5 月 29 日から 6 月 4 日にかけて、第八回 Agda Implementors' Meeting (AIM8) をスウェーデンのイェテボリ市で Chalmers University of Techonology と共同で開催しました。去年 11 月の千里サイトでの AIM7 につづく今回の AIM8 には、CVS4 名、Chalmers9 名、その他 4 名程度の Agda コミュニティーの研究者が参加しました。

CVS は、前身の研究ラボ時代の 2003 年から対話型証明支援系 Agda（ニュースレター第 7 号）の開発に関して Chalmers 大と研究協力をすすめています。年に二回、日本とスウェーデンで交互に行われる AIM 研究集会が協力活動の中心です。通常の研究集会が研究発表セミナーで終わりがちなのに対し、AIM ではそれに加えて「コードスプリント」とよぶ複数のミニプロジェクトを一週間の集中合宿のようにしてやり遂げ、その場で Agda を実質的に発展させることを大きな特徴としています。

今回のセミナー部分では、Agda の実装について 2 件、適用について 4 件、今後の発展に向けた技術と理論について 2 件の発表がありました。CVS からは、矢田部研究員が新論理の Agda による実現、安部研究員が CPU 仕様形式化とテスト生成についてそれぞれ報告しました。後者は、産学共同の研究に関するもので、企業技術者による Agda の受け入れ、産業側が評価する点などについて、大いに Chalmers 側の興味を引きました。

コードスプリントの主要な成果は、第二版 Agda のリファレンスマニュアル整備の枠組みが確立され執筆がはじまったことと、Agda 型理論に「コデータ」型が導入され実装されたことです。

産業への普及をミッションとする CVS としては初版 Agda の時からドキュメンテーションを重視してきましたが、第二版について早期から Chalmers 側と意識をあわせられたことはおおきな意義をもちます。

コデータ型の導入は、Agda を先行する関連システム Coq に追いつかせさらに Agda 流の利点を加えるものです。その他、コンパイラーやライブラリ拡充のミニプロジェクトが実施されました。

近郊のイェテボリ群島への遠足風景

また、今後の進展が話し合われ、うち一つの第二版 Agda へのプラグイン拡張機能について、実装方針の合意を受けて CVS が開発をすすめています。

日本での次回 AIM9 は、11 月 27 日から 12 月 3 日、はじめて千里をはなれ仙台で開催するべく準備中です。JST 国際強化支援策の支援も受けて、AIM の特徴を維持しつつよりオープンなものとし、Agda 関連研究の普及にも力点をおきます。同時期に仙台で開かれる証明支援系関連集会参加者をはじめ多くの皆様の参加をお待ちします。

AIM9開催のお知らせ

日程:2008年11月27日(木)～12月3日(水)
場所:フォレスト仙台 2階会議室
主催:産業技術総合研究所システム検証研究センター
共催:科学技術振興機構
詳しくは当センターホームページをご覧ください。
http://unit.aist.go.jp/cvs/

DSW'08 開催報告

主催：日本ソフトウェア科学会 ディペンダブルシステム研究会
共催：産業技術総合研究所 システム検証研究センター

7 月 2 日から 4 日にかけて、函館大沼にて第 6 回ディペンダブルシステムワークショップ（DSW'08summer）が開催されました。昨年と同じく、函館大沼プリンスホテルにおいて合宿形式で行われ、参加者全員に発表をして頂いたことからか活発な議論が交わされました。

会場付近の大沼公園

とくに、システム開発の分野と検証の分野の研究や企業の方々など、専門の異なる人々の間で内容の濃い交流が出来たと考えます。

一般公開　開催報告

2008年7月25日(金)
尼崎事業所において
「一般公開」が開催され
当センターでは
LEGOを用いた簡易
プログラム体験
コーナーと「筆算の
からくり」と題し
講義を行いました。
来場者数は３５７名で
成功裡に終了しました。

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●イベント・講演会

2008年3月～2008年7月

イベント開催報告

◆計算機言語談話会(CLC)　毎週木曜日開催

日付　講演者(所属)

3/27　矢田部俊介(産総研CVS)

4/10　木下佳樹(産総研CVS)

4/17　木下佳樹(産総研CVS)

6/12　蓮尾一郎(京都大学数理解析研究所)

6/26　田口研治(国立情報学研究所)

〔開催場所:産業技術総合研究所　システム検証研究センター
千里オフィス6F会議室〕

直近のスケジュールはこちらから▼

CLCのURL:http://unit.aist.go.jp/cvs/CLC/

◆システム設計検証技術研究会　２ヵ月毎に開催
(産総研コンソーシアム)

第一回　6月19日開催

講演者　有馬仁志氏　(dSPACEJapan株式会社代表取締役社長)

デモンストレーター：
クリスチャン バウアー氏、太田代優氏、吉岡大助氏

演　題　「Hardware-In-the-Loop Simulation (HILS) による制御ロジックの検証と自動車制御開発での発展」

概　要　１台の自動車に搭載される、いわゆる車載コントロールユニット(ECU)と実装されるソフトウエアは、安全・環境対策にかかわる部分だけでな く、車両機能の増大と快適装備の要求により年々高機能化、ネットワーク化している。それとともに車載ソフトウエアの検証に必要な工数も増大しており、安全 確保や品質向上、期間の短縮化、コストの面から新たな検証方法が求められていた。従来は実車やベンチシステムを使用した検証方法が主流だったが、現在ではHILSを使用した自動テストを あわせて使用することが業界標準となりつつある。本講演ではHILS の概要を簡単に紹介。また自動車制御開発にかかわるHILSによるECUと実装ソフトウエアの検証の実例を挙げ、HILS のメリットやトレンドについて説明する。

〔開催場所:　産業技術総合研究所　システム検証研究センター
千里オフィス6F会議室〕

直近のスケジュールはこちらから▼

コンソーシアムのURL：http://unit.aist.go.jp/cvs/con-top.html

デモンストレーション中のクリスチャンバウアー氏

出版

◆テクニカルレポート

4 月発行

PS-2008-010

Yoshinori Tanabe, Koichi Takahashi, Masami Hagiya

A Decision Procedure for Alternation-free Modal μ-calculi

PS-2008-009

Yoshinori Tanabe, Toshifusa Sekizawa,

Yoshifumi Yuasa, Koichi Takahashi

Pre- and Post-conditions Expressed in Variants of the Modal μ-calculus

3月発行

PS-2008-008

Yoshiki Kinoshita, Toshinori Takai

フォーマルメソッドのフィールドワーク

PS-2008-007

Shunsuke Yatabe

再帰的定義を可能にする述語論理の証明支援系上の実装

(Preliminary Version)

PS-2008-006

システム検証研究センター

２００７年度(平成19年度)研究報告集

※テクニカルレポートはHPから入手可能です。

URL：http://unit.aist.go.jp/cvs/techrep.html

編集・発行：独立行政法人産業技術総合研究所
システム検証研究センター
連　絡　先：〒 560-0083
大阪府豊中市新千里西町 1-2-14
三井住友海上千里ビル 5F
Email：informatics-inquiry@aist.go.jp