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
3
2006.03

フィールドワークのシナリオ

産総研が発足してから 5 年、CVS 発足以来 2 年が経ち、我々がフィールドワークと呼んでいる社会との連携活動も新しい局面を迎えつつあるようにおもう。ここで、フィールドワークを、我々がどのようなシナリオで進めようとしているのかを、紹介しておきたい。

◆フィールドワークとは

フィールドワークという語はもともと民族学などでの専門用語で、野外研究と翻訳される。村落などの社会を観察し、それを説明する枠組をつくる研究、といってよいだろう。我々はこの言葉にかなりの拡大解釈をくわえて、科学者が自らの専門知識と技能を用いて一般社会ではたらく意味にもちいている。フィールドワークをとおして社会に貢献するだけでなく、その経験から科学研究の新しい豊かな対象をうみだすことができるかもしれないとの期待をもっている。

◆ 参加者に資するもの

我々がフィールドワークにもとめるものは、具体的な事例にふれることである。検証技法にかぎらず、ソフトウェア開発技法を大規模な開発に適用するには、研究室内の実験では十分ではない。フィールドワークはまた、我々の科学研究におけるテーマ選択にもよい影響をあたえるだろうと期待される。学術の世界にとじこもるだけではなく、社会と相互作用しつつすすむ科学研究を目指す我々にとって、フィールドワークは、外界との接点として重要である。

他方、共同研究のパートナーが、フィールドワークからえるものは、自らの仕事に適応した形での技術移転である。数理的技法を導入するには、教科書にかいてあるような知識だけではたりない。基礎的な知識を、その場その場に適応した形に定型化する必要があるだろう。また、現場の技術者が新しい技法をまなび、新たに発生する作業を身につける必要があるかもしれない。フィールドワークにおいては、研究者が最新の技術をその適用現場に沿った形にして提供することができる。

◆具体的な課題提示

数理的検証法に関係しそうな具体的な課題を、フィールドが CVS に提示するところから、フィールドワークがはじまる。数理的検証法がその課題に有効なのかどうか、前もってフィールドの側でわかるわけではない。それが判断できるようなら、研究所からの技術移転は必要ないのである。ちなみに、検証には直接関係しない開発現場の専門用語や概念を CVS の研究員が理解する必要があるが、それは容易ではない。フィールドが研究所を持っておれば、開発部門と CVS の間の通訳としてはたらくことができて好都合である。

課題が具体的かつ詳細に CVS の研究員の前に提示されたら、モデル検証法、対話型検証法など、多数ある数理的検証技法のうちのどれを用いるべきかを研究員が検討してきめ、それをフィールドの現場に適用する。現場への適用が肝心である。現場が、新しいテクニックを利用することに対して肯定的にならないと、この段階がすすまない。

◆縁側から奥座敷へ

大抵は、CVS が縁側に入れてもらうことからはじまる。初めての適用では、既に開発が終了しているソフトウェアや、昔作ったプロトタイプなどに対する検証をおこなってみせることからはじまることがおおい。記録にのこっている不具合が、数理的検証法でみつかるかどうかをみたりもする。

これをくりかえすうちに、CVS の研究員および数理的検証法へのフィールドの人々からの信頼が増し、次第に縁側から奥座敷へととおしてもらえるようになる。奥座敷とはすなわち、フィールドにおける本格的開発計画、企業であれば、待ったなしの納期が設定されているような開発案件である。そこでフィールドワークを行えるようになって初めて、技法を現実の大規模開発に適用するときの問題点が明らかになり、必要な研究を追加したり、技術者の教育方針を修正したりといったアクションをとることができる。

以上は、これまでの経験を反映したもので、実際に則したものだと自負している。今後、いくつかのフィールドワークを、このシナリオをもとにすすめていきたい。。

システム検証研究センター長　木下佳樹

＜ＣＶＳニュースレター　３号＞
◆ フィールドワークのシナリオ　1P
◆産総研ワークショップ「機能安全規格と適合認証」　2～4P
◆第一回 Agda-CAL ワークショップ開催報告　5P
◆ CVS 研修コースからのお知らせ　5P
◆ イベント・講演会　6P

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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●トピックス 1

産総研ワークショップ

「機能安全規格と適合認証 -IEC61508 のさらなる理解に向けて -」開催報告

産総研ワークショップ「機能安全規格と適合認証」は、2006 年 2 月 8 日に産業技術総合研究所関西センター（大阪府池田市）にて、137 名という多くの皆様にご参加いただき、盛況のうちに終了いたしました。制御機器メーカ、自動車機器メーカを中心に、組込みソフトウェア業界、大学、研究機関からも多数のご参加いただきました。関西のみならず、中部、関東など遠方からも足を運んでいただきました。機能安全に対する関心が大きく広がっていることを改めてうかがわせるものでした。

当日は、朝 10 時に開会、予定通り 9 件の講演およびビジネスミーティングが行われ、午後 6 時過ぎに閉会いたしました。講演での活発な質疑応答だけでなく、休憩時間中や昼食時にも積極的な意見交換が行われました。また、閉会後に開催された交流会にも多くの皆様のご参加をいただき、遅くまで議論が続きました。丸一日をかけてのワークショップでしたので、ご参加いただいた皆様は、さぞかしお疲れだったことと存じます。しかしながら、機能安全に関するワークショップで、これだけの規模で開催されたものは国内では例がなく、充実した一日を過ごしていただけたものと思います。

ワークショップ開催にあたって

詳しいご報告に入ります前に、産総研関西センターならびに当研究センターが今回のワークショップを開催した主旨をご説明いたします。IEC61508 では、ソフトウェアの安全性を確保するための技術として、formal methods（形式的技法）をはじめとするソフトウェア工学の種々の技法が推奨されています。こうした技法を集中的に研究している国内最大規模の研究組織が産業技術総合研究所システム検証研究センター（CVS) です。CVS では経済産業省産業技術環境局認証課、産業技術総合研究所計測標準研究部門などと連携しつつ、社会的国益確保の観点から IEC61508 に関する調査研究を開始いたしました。今回はその活動の一環として、関連する業界や団体から講演者をお招きし、ワークショップを開催する運びとなったものです。

機能安全の 3 つの切り口

機能安全と一口にいっても様々な視点が考えられます。本ワークショップでは、機能安全に対する 3 つの切り口から講演全体を 3 部構成とし、一線で活躍されている方々をお

IEC61508 とは

IEC61508 では、電気・電子・プログラマブル電子技術を用いた安全関連系の安全性能を機能失敗確率に応じて 4 つの水準に区分しており、これを「安全度水準」(Safety Integrity Level; SIL) と呼んでいます。そして安全度水準を満足する安全関連系を実現するためのいわばベストプラクティスとして「全安全ライフサイクル」を規定し、リスク解析、設計から、実装、運用、保守、廃棄に至るまでの規範的手順を示しています。加えて、ハードウェアおよびソフトウェアの設計・開発において用いるべき技術や手法のリストが示されており、安全度水準に応じて選択して適用することが要求されています。

このように、安全関連系の性能を安全度水準という指標で統一的に規定し、必要とされる水準を達成するための手順や手法について規定している点が、従来の安全規格にはない大きな特徴です。更には、組織における機能安全管理や従事者に要求される適性についても規定しており、総合的で大規模な規格となっています。

規格の対象となるのはコンピュータ技術を用いた安全関連系を使用する全ての産業分野で、例えばプロセス産業、機械、医療機器、鉄道、自動車、航空宇宙、原子力と極めて広範囲にわたります。また、

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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

招きして講演をしていただきました。

◆【第一部】安全と規格の概要

第一部では、「安全と規格の概要」と題し、機能安全規格IEC61508の考え方や内容について、専門家の方々よりご説明いただきました。特に、規格制定の背景、特徴、基本概念、認証スキーム、今後の動向、推奨されている設計手法（特にその一つである形式手法）などについて解説がありました。難解とされるIEC61508ですが、講演者の方々の要点を押さえた説明により、理解が更に深まったことと思います。

東京海洋大学
教授　佐藤吉信氏

日本システム研究所
吉岡律夫氏

産業技術総合研究所
木下佳樹氏

◆【第二部】業界の実情

第二部では、「業界の実情」と題し、プロセス産業、制御機器業界、および自動車業界における機能安全化に対する取り組みについて、現場でご活躍されている方々より、貴重な最新の情報をご提供いただきました。加えて、国内対応の遅れを指摘する意見や、そもそも重要なのは品質と安全を一貫して確保することなのであって、規格対応に振り回されてしまっては本末転倒であるとの問題提起もありました。

東京工業大学
教授　仲勇治氏

IDEC株式会社
日本電気制御機器工業会
藤田俊弘氏

トヨタ自動車株式会社
川名茂之氏

◆【第三部】認証の実態

第三部では、「認証の実態」と題し、認証取得のためのリスク分析支援と開発支援、および認証実務について、実際に業務を担当されている方々より、その詳細をお話いただきました。機能安全に対する認証取得の需要が高まる中で、規格を読むだけではわからない認証取得の実情を垣間見ることができ、参加者の皆様にとっても大きな収穫であったことは間違いありません。

テュフ・ラインランド・
ジャパン株式
Joachim Iden 氏

株式会社シーディー・アダプコ・ジャパン
小西晃輔氏

安全度水準を達成するためには、安全関連系の構成要素（デバイス、センサー、コントローラ、通信ネットワーク、ＯＳ等）や、設計・開発工程で用いられる各種ツール（コンパイラ等）に対しても相応の信頼性が求められています。ですから機能安全規格の普及に伴い、多くの企業が対応を迫られることになります。規格への適合が明らかでない製品は市場から締め出される可能性があるからです。

規格の普及につれて、国内でも認証取得を目指す企業が現れてきており、既に数社がIEC61508の適合認証を受けた製品を発売しています。それに伴い、規格への適合認証を取得する際の課題や問題点を指摘する声が上がっています。そもそも要求事項を理解することが難しい上に、要求事項に対する評価基準が明確でないといった点です。そのため、認証取得を目指す企業側ではどの技法をどの程度まで用いるべきかがわからないし、認証機関や認証者の間でさえ指摘にばらつきがあるのが事実です。

また、現状ではIEC61508に基づく機能安全の認証機関がイギリスやドイツの企業に限られており、国内の企業が認証を取得するためにはそうした在欧の企業に依頼せざるを得ないため、掛かる費用や言葉の違いが大きな問題となっています。そのため、日本型の認証基準による国内認証機関の設立への要求もあります。

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
●尼崎サイト：〒661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

活動の今後を語る
－ビジネスミーティング－

◆活動の推進

9つの講演の後、ビジネスミーティングと題して、今後の活動についての全体討議を行いました。ミーティングは、木下研究センター長による問題提起から始まりました。分野や業種を超えた取り組み、安全に関する規格とは独立した議論、そして規格に対する情報科学からのアプローチが重要であり必要であるとの提言がありました。

これに対して、会場からは、機能安全に対する取り組みを進めていく上で、産業技術総合研究所の主導による分野横断的組織の立ち上げを望む意見がありました。特にソフトウェアの安全性について、日本での研究はまだまだこれからであり、本格的な研究を促進するために関連学会に研究部会を設立してはどうかとの声もありました。

◆機能安全認証のあり方

さらに、国内での機能安全認証のあり方についても、議論が及びました。国内での認証機関設立は必須との意見もあれば、国際規格へ日本の意見を反映させるほうが先との意見もありました。より広い視点からは、機能安全規格をめぐる欧州と日本の風土や国策の違いを指摘する声や、機能安全やIEC61508ありきとして議論するのではなく、最終的な受益者の利益をどう確保するかという視点が重要との意見もありました。

◆さらなる議論の必要性

こうした様々な意見を受け、産総研システム検証研究センターでは、今後の活動の方向性を提案していきたいと考えています。しかし、まだまだ始まったばかりの活動ですので、具体的な提案にはさらなる議論を重ねていく必要があります。CVSは、今後もこのような活動を通じて、機能安全分野、広くはソフトウェア認証分野への貢献を果たしていきたいと考えております。


産総研ワークショップ

機能安全規格と適合認証
－IEC61508のさらなる理解に向けて－

プログラム

09：30　開場
10：00　開会挨拶　[illegible]
10：05　ご挨拶　[illegible]

●第一部　安全と規格の概要●

10：10～10：55　基調講演1
「機能安全規格制定の背景と最近の動向」
佐藤吉信　東京海洋大学

10：55～11：40　基調講演2
「機能安全規格 IEC61508 とその認証」
吉岡伸夫　日本システム安全研究所

11：40～12：10　「機能安全規格の中の formal methods」
木下佳樹　産業技術総合研究所システム検証研究センター

12：10～13：20　－昼食－

●第二部　業界の実情●

13：20～14：00　「プロセス安全管理と IEC61508」
仲　勇治　東京工業大学

14：00～14：30　「産業オートメーションにおける制御安全技術の動向と機能安全認証に関する日本電気制御機器工業会（NECA）の取り組み」
藤田俊弘　IEC 株式会社、日本電気制御機器工業会

14：30～15：00　「自動車業界の機能安全標準化動向」
[illegible]　トヨタ自動車株式会社

15：00～15：15　－休憩－

●第三部　認証の実態●

15：15～15：45　「機能安全規格と SIL 評価」
[illegible]　株式会社東芝　電力・社会システム社

15：45～16：15　「安全に関わる制御装置の TÜV 認証」
Joachim Ides　テュフ・ラインランド・ジャパン株式会社

16：15～16：45　「IEC61508 に沿った安全なソフトウェア開発における SCADE の有効性」
小西晃樹　株式会社シーディー・アダプコ・ジャパン

16：45～17：00　－休憩－

17：00～17：50　ビジネスミーティング－今後の活動に向けて－
司会　水口大知　産業技術総合研究所システム検証研究センター

●閉会・交流会●

17：50　閉会挨拶
18：00　交流会

適合認証
機能安全規格

独立行政法人
産業技術総合研究所

主催　独立行政法人産業技術総合研究所　関西センター／システム検証研究センター　日時　平成18年2月8日（水）10：00～18：00
協賛　[illegible]　会場　[illegible]

最後になりましたが、今回の産総研ワークショップにご参加いただきました皆様、講演者の皆様、開催にあたってご尽力をいただいた皆様に厚く御礼申し上げます。

2006年2月
産業技術総合研究所
システム検証研究センター
水口大知

[編集より]

システム検証研究センターでは、今回の産総研ワークショップのような、様々なワークショップを随時開催しております。開催については、WEBにてご案内しております。

URL：http://unit.aist.go.jp/cvs/workshop/

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
●尼崎サイト：〒661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●トピックス 2

第 1 回 Agda - CAL Workshop 報告

1 月 27 日に第 1 回 Agda - CAL Workshop が開催されました。Agda は CVS がシャルマース工科大学（スウェーデン）と共同で、また CAL は京都大学の佐藤雅彦教授グループで、それぞれ開発中の対話型証明支援系の名称です。

木下研究センター長が今ワークショップをよびかけた趣旨は、フォーマルな発表では充分な相互理解が得られないので、証明作業を共有することで両者の理論体系・実装を深く理解し、突っ込んだ討議をしよう、というものです。初回である今回は当研究センターの千里オフィスが会場となりました。参加者は、京都大学より 5 名、CVS より 8 名でした。

CAL は佐藤教授の Natural Framework の理論を実現したもので、現在大学教育に活用され既に 10 年近い実績があります。Agda は Martin-Löf 型理論にもとづき、シャルマース大での二十年来の支援系研究の流れを汲むものです。CVS は 2004 年から開発に加わり、検証への適用研究、改良、次世代 Agda2 開発などで活動しています。

当日は 10：00 に全員集合。共通課題「加算が数の大小関係を保存することを、数の定義からはじめてあらゆるやり方で証明してみる」の資料配布とともに「では、作業にかかって下さい」という開会宣言で始まり、12:00 まで、皆一身不乱でコンピュータに向かいキーボードを叩いていました。日頃愛用のシステムとはいえ、なかなか思うように証明が進まないのも常。時には溜息も。あっという間の 2 時間が経ち、昼食のため作業を中断しました。昼食後は、13:30 より再開、まず両グループから各々のシステムの紹介があり、質疑応答がなされました。その後、15:30 から 17:00 まで各自が仕上げた証明を互いに披露し、皆で吟味しました。専門的には、再帰的／帰納的述語定義、帰納法の扱い、証明構成操作の技法・実装などについての比較検討がトピックでした。

共同作業を通じて双方の理解が進んだため、打ち解けた雰囲気の中で、活発な質疑応答がなされ、当初の目的は達成されました。とても実りある Workshop であったと思います。両グループの再会を約束し、閉会となりました。

●お知らせ

モデル検査研修コース（初級）の本格的開始についてのお知らせです

これまで約一年にわたって、モデル検査研修コース (初級) の教材開発のために、CVS が研修コースを無料試行してまいりました。受講生のご意見をもとに教材の改良を重ね、このたびモデル検査研修コース (初級) が一応の完成をみましたので、その試行を終了いたします。

CVS は以下の研修コース教材をさらに開発中です。開発中の研修コースについては、無料試行を行って、教材の改良を重ねております。

	モデル検査	対話型検証
初級	開発済	開発中
中級	開発中	開発予定
上級	開発中	開発予定

開発を完了した研修コースの本格運用は、CVS 認定の外部機関に移管いたします。当面、株式会社システム検証研究所が研修コースを運用してまいります。

モデル検査研修コース (初級) の本格運用についての問い合わせ先
株式会社システム検証研究所
Email: inquiry@svvlab.com
URL : http://www.svvlab.com

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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●イベント・講演会

2005 年 12 月～ 2006 年 02 月
イベント開催報告

◆計算機言語談話会（CLC）　毎週木曜日定期開催中

日付	講演者（所属）
11/24	亀山幸義（筑波大学）
12/01	尾崎弘幸（CVS）
12/15	松岡聡（AIST 計測標準部門、CVS）、水口大知（CVS）
2006 年	
01/12	青戸等人（東北大学、電気通信研究所）
	千葉勇輝（東北大学）
01/19	大﨑人士（CVS）
02/02	高井利憲（CVS）
02/09	Moonzoo Kim
	（Pohang Univ. of Science and Technology）
02/23	Georg Struth（The Univ. of Sheffield）
02/27	近山隆（東京大学）

（開催場所：システム検証研究センター千里サイト）

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 ヶ月毎に開催中
（産総研コンソーシアム）

第四回　2005 年 12 月 20 日開催

講演者　石井通義、苅部慎介（日本アイ・ビー・エム株式会社）

演　題　「手書きによるコード記述から UML モデリングによるコード生成へ　IBM Rational RoseRealTime」

第五回　2006 年 1 月 26 日開催

講演者　黒瀬美宏（日本アイ・ビー・エム株式会社）

演　題　「最新の管理手法による製品品質の追跡　IBM Rational が提案する統一変更管理（UCM）」

第六回　2006 年 2 月 16 日開催

講演者　穴田啓樹（キャッツ株式会社）
松本充広
（福岡県産業・科学技術振興財団福岡知的クラスター研究所）

演　題　「状態遷移表モデル検査の概要と検査ツールの紹介」

（場所：システム検証研究センター千里サイト）

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/consortium/

◆ワークショップ　随時開催中

第一回 Agda-CAL　Workshop　　2006 年月 1 日 27 日

（場所：システム検証研究センター千里サイト）
※詳細は本ニュースレター 5P をご参照ください。

産総研ワークショップ

「機能安全規格と適合認証 -IEC61508 のさらなる理解に向けて」
2006 年 02 日 08 日

（場所：産総研関西センター）
※詳細は本ニュースレター 2-4P をご参照ください。

◆研修コース

2005 年 12 月 12 日～ 15 日
第 10 回モデル検査研修コース初級編（NuSMV）

2006 年 01 月 16 日～ 19 日
第 11 回モデル検査研修コース初級編（NuSMV）

（場所：システム検証研究センター千里サイト）

直近のスケジュールはこちらから▼
研修コースの URL：
http//unit.aist.go.jp/cvs/training-course/training-course-top.html

出版

◆テクニカルレポート

2005 年 9 月発行

PS-2005-016　Koki Nishizawa
” Algebraic Structures for Cocomplete Fibrations and Fibred CCCs”

2005 年 12 月発行

PS-2005-018　Hitoshi Furusawa, Eun-Hye Choi, Hiroshi Watanabe
”Efficiency Analysis of Model-based Review in Actual Software Design"

2006 年 01 月発行

PS-2006-001　Eun-Hye Choi, Tatsuhiro Tsuchiya, Tohru Kikuno
” Model Checking Active Database Rules"

※全てのテクニカルレポートは HP からも入手可能です。
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