基礎研究

形式アシュランスケースの研究

■ 教授 **木下 佳樹** ■ 理学部 ■ 情報科学科

キーワード アシュランスケース、形式アシュランスケース、Agda、オープンシステム・ディペンダビリティ

研究概要

アシュランスケースは、システムの安心・安全に関する確信を得るに至った経過と結果を記録した文書です。認証のための提出文書としてのみならず、システムの利害関係者間の合意事項の記録などとして、近年急速に注目されはじめ、その国際標準も次々に制定されています。大規模で複雑なシステムのアシュランスケースは、膨大な文書です。その内容が適切であることの確信を得るためには、アシュランスケースの全体的な把握と、細部にわたる厳密な理解という、相反する要件が求められます。そのため、我々はアシュランスケースを論理的な形式言語で記述し、様々な意味処理を可能にする『形式アシュランスケース』の研究を行なっています。

GSNによる構造化アシュランスケース

Agdaによる形式アシュランスケース

アシュランスケース文書処理の課題	プログラミング言語処理の課題と解決策
議論の整合性検査	プログラムの型検査
関連アシュランスケースの一括処理	プロジェクトのビルド
大規模アシュランスケースの構造化	抽象化、モジュール化
構成管理	プログラムの構成管理
トレーサビリティ	プログラムの型検査

研究の特徴・比較・優位性

アシュランスケースの理解を助けるために、図式を用いて表現する構造化アシュランスケースが用いられています。しかし、現状ではプログラミング言語処理技術の成果が十分に活かされていません。構成的型理論に基づくプログラミング言語Agdaでは、プログラムと論理式を一つの枠組みで記述できます。本研究室では、Agdaでアシュランスケースを記し、整合性検査、トレーサビリティ確保、バージョン管理等のプログラミング言語処理技術による系統的な実現を研究しています。

今後の展望

アシュランスケースは、システムアシュランスの第三者認証における提出文書として各方面に広がりつつあります。システム及びソフトウェアのアシュランスに関する規格ISO/IEC 15026の第2部はアシュランスケースの規格です。木下研究室では現在（2016年1月末)、目的や環境、境界が変化し続けるオープンシステムのための形式アシュランスケース・フレームワーク（FFO）を構築中です。これは制定中のIEC 62853 Open systems dependabilityに基いてディペンダビリティ・アシュランスの客観的な評価法の基盤を与えるものであり、今後このフレームワークに基づく第三者認証の枠組を提供するべく技術展開を図っていきます。

MESSAGE

近年では、システムは他のシステムと互いに接続されるのが当然のようになっています。そのようなシステムでは、対象システムだけではなく、周辺システムのディペンダビリティも考慮に入れることが必要です。総合的アプローチなしには、対象システムのディペンダビリティは向上しません。私は、そのために必要な国際標準IEC 62853 Open systems dependabilityの制定作業をプロジェクトリーダーとして進めています。安心・安全で信頼性の高いシステムの構築を目指す企業等との連携が必要です。

INFORMATION

研究プロジェクト(相手先/研究種別/研究題目)：

1. (独)情報処理推進機構/受託研究/オープンシステム・ディペンダビリティのための形式アシュランスケース・フレームワーク
2. (株)デンソー /共同研究/自動車機能安全ケースの為のフレームワークに関する研究
3. 平塚市/共同研究/平塚市地域防災計画の整合性検査方式の研究
4. (国研)産業技術総合研究所/共同研究/有機化合物のスペクトルデータベースシステム(SDBS)の帰属、及び、帰属決定プロセスについてのアシュランスケースの研究

問い合わせ先：産官学連携推進課　神奈川県横浜市神奈川区六角橋3-27-1　TEL：045-481-5661(代)　sankangaku-web@kanagawa-u.ac.jp