「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」

H23 年度
実績報告

平成 20 年度採択研究代表者

木下佳樹

産業技術総合研究所
情報技術研究部門（2011.6 まで組込みシステム技術連携研究体）
主幹研究員

利用者指向ディペンダビリティの研究

§1. 研究実施体制

(1)「木下」グループ

①研究代表者:木下　佳樹　（産業技術総合研究所情報技術研究部門、主幹研究員）

②研究項目

1. 開放情報系ディペンダビリティの概念確定
2. 開放情報系ディペンダビリティに関する規格制定
3. 適合性評価技術（D-Case）
4. ライフサイクル技術ガイドライン

§2. 研究実施内容

(文中に番号がある場合は(3－1)に対応する)

木下チームは全体で一つのグループとして活動している他、23 年度は DEOS プロセス/アーキテクチャ会議および標準化サブコアチームと連携しながら活動した。4 つの研究項目についてそれぞれ研究のねらい、これまでの研究の概要、研究進捗状況、研究成果、今後の見通しを説明する。

(2－1) 開放情報系ディペンダビリティの概念確定

(2－1－1) 研究のねらい

利害関係者間の前提が異なることによる齟齬が生じやすいという問題意識から、本年度は合意形成過程を明確にする研究を行った。

(2－1－2) これまでの研究の概要

合意形成のダイナミズムを生むのは、D-Case 文書に対する反論 (rebuttal) であると考えられる。少なくとも一旦は合意の対象となった D-Case 文書が変更されるとすれば、どこかに矛盾あるいは不適当な箇所が認められるからである。そのような箇所を指摘することは、D-Case 文書への一種の「反論」であるとみなされる。D−Case の内容のように、信頼性や安全性など、唯一絶対の真理ではなく、物事に関する判断の論理を研究する「議論の理論 (argumentation theory)」では、反論は研究対象の中心の一つであるが、それを情報科学の立場から研究するために、以下の四項目を計画した。

①D-Case の主張に対する反論(rebuttal)とそれを受けての修正とは、どのようなことなのかについての論理的分析とその支援システム
②合意形成の過程の D-Case による表現とその支援システム
③D-Case 文書のトレーサビリティの分析とその支援システム
④視点による D-Case 射影の分析とその支援システム

(2－1－3) 研究進捗状況

Dung は、反論を議論の間の二項関係であるとの前提から出発して、自らの反論がすべて逆に反論されている「容認できる」議論の構造の一般論を研究し、容認可能性を論理プログラミングで判定する方法などを与え、議論の研究において Dung の議論モデルと呼ばれている。①②に関して、Dung の議論モデルを D-Case/Agda の枠組みに適用する研究を開始した。③④の構築開始にはまだ至っていない。

(2－1－4) 研究成果

D−Case に対する rebuttal を Dung の議論モデルに基づいて解析した結果([10])を発表した。

（2－1－5） 今後の見通し

D-Case に関する rebuttal の現在の解析結果に改良の余地がある。Dung の議論モデルが Default logic に適用されたのと同様に、今後、同モデルを D-Case/Agda が立脚する直観主義論理に適用し、D-Case/Agda の記述に対する反論の理論的根拠を与える。

（2－2） 開放情報系ディペンダビリティに関する規格制定

（2－2－1） 研究のねらい

Open Systems Dependability の概念の規格化は IEC TC56 Dependability で行う。ISO/IEC JTC1 SC7 Software and System Engineering ではシステムアシュランス（ディペンダビリティに強く関係し、米国で使われはじめた語）に関する先行活動に Open Systems Dependability の概念を注入する。また、D-Case 周りのツールにつながる規格を OMG System Assurance Task Force で構築する。

（2－2－2） これまでの研究の概要

IEC TC56 では Open Systems Dependability の概念の説明を国内委員会で繰り返し、浸透を図った。ISO/IEC JTC1 SC7 WG7 では ISO/IEC 15026 Systems and software assurance に Open Systems Dependability の概念を導入する努力を続けた。

（2－2－3） 研究進捗状況

ISO/IEC JTC1 SC7 WG7 では、ISO/IEC 15026 System and Assurance Case Part 3 Integrity Levels および ISO/IEC 15026 System and Assurance Case Part 4 Assurance in System Life Cycle の coeditor を派遣して執筆し、前者は IS (International Standard)出版された。いっぽう後者は現在 DIS (Draft International Standard)投票（2012 年 6 月投票締切）に付されている。この規格案は、システムライフサイクルの各過程で high assurance (= dependability)実現のために何を行うべきかについてのガイダンスを記したもので、我々の計画にとってはテーマ 1.4 の主要な成果ともなる。

IEC TC56 では、Open Systems Dependability の概念を記した新しい規格策定の NWIP (New Work Item Proposal)を WG4 System Aspects of Dependability に提出することを計画し、24 年度初頭の提案を目指していたが、国際委員会での手続き的理由により遅れており、現在 24 年 7 月の提案を見込んでいる。一方、「少なくとも五カ国から、規格案にコメントを寄せる expert が派遣されること」という新規案件開始の条件が満たされないために規格制定プロジェクトが成立しない場合も多い。これに備えて、米国、英国などの識者に expert 依頼を受諾するよう働きかけた。

OMG (Object Management Group)の System Assurance Task Force には、D-Case/Agda が他に先駆けて実現している assurance case の整合性検査の機能について、それを可能にする

ための言語機能を規格化する計画 MAC (Machine-checkable Assurance Case)を、本年度新たに開始することとした。

(2－2－4) 研究成果

本年度の研究の最も顕著な成果は ISO/IEC 15026-3:2011 の出版[17] である。3 名の editor (Project editor: S. Redwine, coeditor: 高井利憲と Karen Richter)のうちの 1 名を本プロジェクトから派遣した。(学術論文では editor の名は規格文書には記されず、出版されたときに、その規格出版を担当した ISO の Working Group の公式記録にその名を記してその貢献が記録される。しかし公式記録の配布は規格文書とは独立で広範囲にわたらないので、本プロジェクトの 15026−3 制定への貢献を明らかにするためにこのことを記す。)

(2－2－5) 今後の見通し

IEC TC56 への Open Systems Dependability 要件規格の NWIP (New Work Item Proposal)提出は、2012 年度中に行う。

ISO/IEC JTC1 SC7 WG7 では当面、15026-4 の改訂作業が中心である。同作業は現在、DIS 投票の段階であり、順調に進めば 2013 年中に規格が出版される見込みである。また、WG7 では 15026-3 の再改訂が議論され始めており、再び coeditor を派遣する可能性もある。

MAC の RFI(Request For Information。ISO/IEC における NWIP に相当するアクション)を 2012 年中に OMG System Assurance Task Force 集会に提出する計画である。

(2－3) 適合性評価技術(D-Case)

(2－3－1) 研究のねらい

D-Case の記述による適合性評価法を研究する。本プロジェクトで当初計画していた適合性評価法の研究を、D-Case の記述および評価法の研究として拡張し遂行している。

(2－3－2) これまでの研究の概要

22 年度に D-Case/Agda システムを稼動開始させた。これに伴い、D−Case の様式を Agda 言語におけるデータ型およびその周辺の宣言として定式化した。

(2－3－3) 研究進捗状況

D-Case/Agda を 2012 年 10 月に無償公開、基本的なアイディアに関する特許を申請した。

また、本年度は D-Case/Agda による D-Case 記述方法論研究を開始した。Web による架空の販売サイトの信頼性に関する D-Case 記述、X 社におけるソフトウェアバージョン運用ガイドラインの安全性に関する D-Case 記述などの実験を 2012 年 12 月から 3 月にかけて行った。両実験とも年度末まで続いたので、結果の解析は来年度に持ち越すこととなった。合意形成過程の研究につい

ては(2－1)の通り。

(2－3－4) 研究成果

D-Case/Agda を 2012 年 10 月に無償公開し[16] 、また、それに先立って基本的なアイディアに関する特許を申請した。

(2－3－5) 今後の見通し

適合性評価法については、24 年度はD-Case 記述実験をより広範囲に行う。対象としてファイルサーバのディペンダビリティ、加賀美グループのロボット展示のアカウンタビリティなどを考えている。NASA Ames 研究センターとの研究交流を続ける。

(2－4) ライフサイクル技術ガイドライン

(2－4－1) 研究のねらい

Open Systems Dependability を達成するために、システムライフサイクルの各プロセスでどのようなことをなすべきか、を記したガイドラインを作成することとした。

(2－4－2) これまでの研究の概要

ガイドラインを国際規格 ISO/IEC 15026-4 として標準化している((2－2)参照)。この規格では特に Open Systems Dependability の語は用いていないが、これまでの我々の研究成果を反映させている。一方、我国の産業界作成の、「IT 化の原理原則 17 ヶ条」にも、open system の立場から見て重要な条項が多数含まれているので、15026-4 執筆にとりいれた。

(2－4－3) 研究成果

主たる成果物は ISO/IEC 15026-4 の規格となる予定である。現在 DIS 投票に付される段階である。また、「IT 化の原理原則 17 ヶ条」の英訳に協力した。

(2－4－4) 今後の見通し

順調にすすめば 2013 年中に ISO/IEC 15026-4 が出版される見込みである。

§3. 成果発表等

(3－1) 原著論文発表

・論文詳細情報

[1] Takafumi Komoto, Kenji Taguchi, Haralambos Mourtidis, Nobukazu Yoshioka and Kokichi Futatsugi, A Modelling Framework to Support Internal Control, Companion of 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement, 6, 2011

[2] *Yutaka Matsuno and Kenji Taguchi, Parameterised Argument Structure for GSN Patterns, Proceedings of the 11th International Conference on Quality Software, 7, 2011
Assurance caseの記法にパラメータを導入する試みを行った。

[3] Hiroyuki Kido, Katsumi Nitta: Toward Justifying Actions with Logically and Socially Acceptable Reasons, Lecture Notes in Artificial Intelligence, Proc. of 10th Mexican International Conference on Artificial Intelligence, Part 1, 7094, pp. 52-64, 2011.

[4] 大畠明, 田口研治, 松野裕, 中坊嘉宏, 消費者機械安全性・信頼性保証の国際標準化, SEC Journal, 7, 4, IPA, 1, 2012

[5] 木藤浩之, 新田克己: Pareto最適な撤回可能帰結を軽信的に正当化する実践的議論意味論, 人工知能学会論文誌, Vol. 27, No. 2, pp. 52-60, 2012.

（3－2） 知財出願

① 平成 23 年度特許出願件数(国内 1 件)

② CREST 研究期間累積件数(国内 1 件)