

「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」

H22 年度 実績報告

平成20年度採択研究代表者

木下佳樹

(独)産業技術総合研究所 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. 研究実施の概要

ディペンダビリティに関するこれまでの議論で欠けていたと思われる、開放系に関するディペンダビリティの概念を明確にし、プロセスやアーキテクチャとして提示し、標準化することが、本チームのミッションである。概念の明確化については、オープンシステムディペンダビリティ(OSD)の概念を規定する論文を執筆し、投稿準備中である。また、国際標準規格活動については、ISO/IEC 15026 System and software assurance の新版作成に、本チームから共編者が参加し、OSDの概念を盛り込みつつある。プロセスやアーキテクチャに関しては、D-Case ツールの基本概念を提供し、開発に参加している。また、企業との共同研究を通じてD-Caseの記述事例を作成する技術適用実験の準備を進めている。

§2. 研究実施体制

(1)「木下」グループ

① 研究分担グループ長:木下 佳樹 (産業技術総合研究所 組込みシステム技術連携研究体、主幹研究員)

② 研究項目

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

§3. 研究実施内容

(文中に番号がある場合は(4-1)に対応する)

① 【開放情報系ディペンダビリティの概念規定】

利用者指向ディペンダビリティと開放情報系ディペンダビリティを合成させた形で概念を明らかにした。本年度の研究を通じて

(ア) 開放情報系ディペンダビリティを論じなければならない背景には、

- 1) 予測不能(何が起こるか分からない)
- 2) 利害関係者間の意思疎通の齟齬
- 3) 経時的変化への追従の必要
- 4) 全体像の把握が困難なこと

などの課題があること

(イ) 上記課題解決のためには

- 1) 危機管理、
- 2) 合意形成

の二つが重要であること

などを明らかにした。現在執筆中のその内容は、サブコアチームにおける議論を通じて領域全体に浸透しつつあり、DEOS ホワイトペーパー第二版にも内容が反映されている。

② 【開放情報系ディペンダビリティに関する規格制定】

規格化においては、ISO、IEC におけるデジュール規格および OMG におけるデファクト規格の双方で活動した。

(ア) ISO/IEC JTC1 SC7 system and software engineering において ISO/IEC15026 System and software assurance の改訂の coeditor を高井(part 3)と木下(part 2 and part 4)が務めている。System assurance とはシステム高信頼性の意味であり、dependability あるいは最近いわれる resilience と同じの内容である。実際、本プロジェクトの D-Case の考えを part 2 (assurance case) に反映させた。part 2 は 2011 年 2 月に発行された。また、part 3 は FCD を完成させた。

(イ) IEC TC56 dependability において、open information systems dependability に関する NWIP (new work item proposal) を提案するべく、WG4 国内委員会および convener (D. Kiang) と交渉した。その結果、国内委員会の了解をとりつけ(9 月)、国際委員会の convener も、ポジティブである(10 月の plenary meeting で交渉)。2011 年 4 月の interim meeting で内容説明の機会が与えられる予定で、その後準備のち、2012 年春の NWIP 提出を目標に活動を進めている。

(ウ) OMG(Object Management Group)の system assurance task force において RM

(Argumentation Metamodel) と SAEM (Software Assurance Evidence Metamodel) を SACM (Structured Assurance Case Metamodel) に統合する活動を行った。

③ 【適合性評価技術 (D-Case, assurance case)】

適合性評価法として D-Case の記述および論理的分析による適合性評価法を研究した。Assurance case の巨視的なレベルでの整合性を定理証明技術で検査する手法を開発し、サブコアチームが開発している D-Case エディタと産総研が開発に参加してきた定理証明支援系 Agda とを連結し、D-Case エディタでグラフィックに入出力する D-Case の整合性を Agda で検査する環境を作成し、開発版を研究領域内で試用評価している。これに関連してシステムの利害関係者間のリスクコミュニケーション支援について考察した(論文4.)。また、D-Case の事例収集のため、X 社と共同研究を開始し、同社での安全分析の結果を D-Case に記すことも開始した。本年度は、安全分析の手法および D-Case 記述のメタモデル構築を行った。一方、Common Criteria に基づく security case およびセキュリティに関する要求分析に関するモデル構築を行った(論文1.)。また、Jackson による要求仕様の妥当性確認と仕様の管理について考察した(論文4.)。

【ライフサイクル技術ガイドライン】

ディペンダビリティのアセスメントに関する提案を行った3.)。また、ISO/IEC 15026 System and Software Assurance, Part 4 Assurance in Life Cycle の working draft を作成した(S. Redwine, K. Richter と共同)。

§4. 成果発表等

(4-1) 原著論文発表

●論文詳細情報

1. Kenji Taguchi, Nobukazu Yoshioka, Takayuki Tobita, Hiroyuki Kaneko. “Aligning Security Requirements and Security Assurance Using the Common Criteria”, In Proc. Fourth International Conference on Secure Software Integration and Reliability Improvement, SSIRI 2010, Singapore, June 9-11, 2010. IEEE, pp69-77.
2. Yoshiki Kinoshita and Toshinori Takai. “A field-scientific approach to Clinico-Informatics”, Synthesiology English edition, Vol. 3, No. 1, pp.64-76, ISSN 1883-0978 (Print), ISSN 1883-2318 (Online), July 2010.
3. Keishi Okamoto, Yoshiki Kinoshita, Takahiro Seino, Noriaki Izumi, Koiti Hasida and Hiroki Takamura. “A Design for an Assessment Process for Dependability based on a Formal Model”, Proceedings of the IASTED International Conference, Advances in Management Science and Risk Assessment (AMSRA 2010). (in print).
4. Yutaka Matsuno, Jin Nakazawa, Makoto Takeyama, Midori Sugaya, Yutaka Ishikawa. Toward a Language for Communication among Stakeholders. In Proc. The 16th IEEE Pacific Rim International Symposium on Dependable Computing, IEEE. (to appear)
5. Takashi Kitamura, Keishi Okamoto, Makoto Takeyama. Formal validation and requirements management based on the Jackson's reference model for requirements and specifications(Fast Abstract). In Proc. The 16th IEEE Pacific Rim International Symposium on Dependable Computing, IEEE. (to appear)

(4-2) 知財出願

- ① 平成22年度特許出願件数(国内 0 件)
- ② CREST 研究期間累積件数(国内 0 件)