Vol.2009-EMB-14 No.2
2009/7/24

最小セット OS 開発の作業改善と診断

後藤健太郎,柏原一雄,市川知典,竹下千晶*,三輪田寿康,川口直弘**,堀武司***,斉藤直希,小川清****

Process Improvement and assessment for developing a smallest set operating system

Kentaro GOTO, Kazuo KASHIWABARA, Tomonori ICHIKAWA, Chiaki TAKESHITA(DENSO CREATE Inc.) , Toshiyasu MIWATA, Naohiro KAWAGUCHI(SUNTEC inc.), Takeo HORI(Hokkaido IRI), Naoki SAITO, Kiyoshi OGAWA（NMIRI）

キーワード:最小 OS, 作業診断, 国際規格, 適合確認, システム工学

1. 概要

著者らは，最小セット OS の設計作業に対して，Automotive SPICE を含むモデルを用いて作業診断する方法について検討している。最小セットOSの設計作業には，HAZOP[5]，ソフトウェアとハードウェアの協調設計を可能にするための UML[8]を使った状態遷移図の作成，状態遷移図に基づいたモデル検証，実装したコードの MISRA-C による C 言語部分集合への対応などがある。これらの道具としての技術要素を有効に生かした研究試作の作業群に対する診断を計画している。

第2章で技術要素について示し，第3章で診断の基礎となる製品評価，技術者評価，作業評価について ISO/IEC 15504 をはじめとする国際規格に基づいた基本的な枠組みについて紹介し，第 4 章で現在進行中の作業改善と診断の鍵となる視点を示し，第 5 章でまとめと今後の課題を示す。

2 技術要素

2.1 最小セット OS

2007 年に斉藤がμITRON4.0[2]最小セットの実装を日本で最初に発表した。現在，TOPPERS 割り込み処理モデルおよび TOPPERS 統合仕様書への対応の設計変更（設変）を名古屋市工業研究所及び TOPPERS プロジェクト参加企業で検討している。

名古屋市工業研究所および北海道立工業試験場は平成 14 年度 地域新生コンソーシアム事業（経済産業省東北経済産業局）採択の「組込みシステム・オープンプラットホームの構築とその実用化研究」において TOPPERS/JSP カーネル[1]のいくつかの CPU への移植作業に参加した。Renesas 製 CPU M16C/ M32C[3]への移植は，TOPPERS 教育 WG の協力[4]の下に行った。北海道立工業試験場 は SH2 の移植を行った。また，成果に基づき，公的試験研究機関での移植と教育の取組みを進めて来た[7][14]。

最小セット(smallest set profile)は，μITRON4.0 の最低限の仕様を満たすものである。最小セットの特徴は，OSEK[6]の最小構成と同様に，タスクの待ち状態がないことである。

2.2 HAZOP

HAZOP は，流れに沿って故障解析を行う際の経験的な手法である。網羅性にすぐれており，設計の各段階において分析する有効な手法である。最小セットOSの仕様の設計において HAZOP を主作業とすることを計画している。HAZOP の利用の仕方として，システムに関する情報が十分に得られていない段階での作業についても検討している。[26][27]

ISO 9000[10]の自動車向けプロファイルである ISO TS 16949[11]では，IEC 国際規格の FMEA[12], FTA[13]を参照しているが，HAZOP については言及していない。

2.3 UML と振舞い記述としての状態遷移図

システム開発では，ハードウェアも，ソフトウェアも，状態遷移が基本的な要素であることが知られている。CPU は，状態機械として抽象化可能であり，ソフトウェアはその状態を遷移させるための手順の一部である。国際規格にもなった UML には，状態遷移図の規定があり，状態遷移図を含む振舞い記述については，表形式の可能性を示している。

2.4 形式手法とモデル検査

堀による B の利用[28]，斉藤による Z の記述を始めとして，形式的な手法の利用から，仕様書の集合論的な把握の必要性が理解できた。状態を記述するためには，仕様を集合論的に把握する必要がある。そのためには，用語を is-a 関係で規定する必要がある[15]。形式手法に基づいた集合論的な記述については，モデル検査の実施も検討している。

*株式会社デンソークリエイト
**株式会社サンテック
***北海道立工業試験場
****名古屋市工業研究所

2.5 MISRA-C

MISRA-C は，イギリスにおける自動車関連ソフトウェアに関するガイドを発行しているMIRAによるC言語コーディング標準である。MISRA-Cは，言語処理系のC言語国際規格[20]適合を必要としている。C言語国際規格に適合しているだけでは，あいまいなところがあるため，CPU間の可搬性のための部分集合を定義したのが MISRA-Cである。日本語版は，自動車技術会から発行されている。SESSAMEのMISRA-C研究会では，MISRA-Cの内容を検討し，意見交換を行うとともに，具体的な運用方法を含む解説を提案している。MISRA-C 研究会に，デンソー，サンテック，名古屋市工業研究所をはじめとする名古屋地区の企業が参加し，MISRA-C の解説書を作成してきた[17][18]。MISRA-C は言語の部分集合であり，最小セットは，OS としての部分集合であり，方向性に共通部分がある。

名古屋市工業研究所では MISRA-C の解説書のサンプルコードを，TOPPERS/JSP 上で動作させるとともに，Windows 上の Visual C，Linux/cygwin 上の GCC でコンパイル・実行することにより，処理系定義の課題，OS の課題について検討してきた[19]。

3 製品評価，技術者評価，作業評価

3. 1 製品評価

作業評価にあたっては，ISO/IEC 9126[30]，現在のISO/IEC 25000 SQueRE[31]に基づいた製品評価が重要である。ETSS[29]で明確になったように，作業の仕方は技術者の能力に応じて対応することが重要である。作業途中の作業生産物（成果物）を SQuaRE に沿ってプロファイルを作る提案をしている。

3.2 技術者評価（スキル判定）

公的試験研究機関における研修ではC言語の知識のみを前提として1年以内に異なる CPU への移植ができるような人材の育成を目標の一つとして設定した。前提として，大学における卒業研究の一貫として研修を行う場合と，企業で C 言語の経験のある方々への組込み技術者の養成研修の一貫として取り扱う場合を考慮している[21]。これらの研修における知見として，技術者の能力とやる気が，設計作業の内容を大きく規定するものであり，その指標としてはETSSの利用を検討してきた。

ETSS においては能力に応じた作業を基本としている。特に，高度な技術者は，作業の改善を実行できることを示唆している。最小セット設計においては，当初参加の技術者は，すべて水準4であることを前提としている。

スキル表は，IPA/SEC の渡辺登氏の指導のもと，実際の開発，教育の経験を記載することにより，水準の根拠を明確にする方法を取っている。また，機能安全のアセッサのスキル表を統合している。現在形式手法に関するスキル表を別途作成している。今後は形式手法のスキルとの統合も検討している。

3.3 作業診断（process assessment）

ISO/IEC 15504[16]の情報源のひとつであるCMM[32]を作成した SEI は，ISO/IEC 15504 に基づいたCMMI[33]としての改定を行っているほか，PSP[34],TSP[35]など個人やチームの仕事の仕方に焦点を当てている。また，IEEE では人の能力の判定に焦点をあてている。IEEEが提案し，IPAの向山博がエディタをして作成したソフトウェアの専門化評価の仕組みのガイド[36]がある。

ISO/IEC 15504 は 1998 年に TR を発行し，2003 年にpart2 が国際規格になった。ISO/IEC 12207[37]に基づく診断モデルの例であるISO/IEC 15504 part5 が2004年に国際規格になった。ISO/IEC 15504 の規格制定においては，日本が最も多くのエディタを出している。小川清はpart2, part6,現在審議中の part9 のコエディタをしており，規格の適用範囲，適用の仕方についての課題を検討してきた。日本の ISO/IEC JTC1 の National Body では，ISO/IEC 15504 の投票においては，用語と概念を規定した part1 を除き，例であるので国際規格ではなく，継続してTRとすることを主張して反対している。2008年には，ソフトウェアを含むシステム開発のプロセス定義[38]に基づくISO/IEC TR 15504 part6を発行している。

Part5, part6のどちらも，修整プロセスを定義しておらず，モデルをどのように修整したか，国際規格に適合したモデルとは何であるかが必ずしも明確にはなっていない。そのため，現在ISO/IEC JTC1 SC7において，conformity assessment に関するガイドを検討している。

4 作業改善

3.1 作業診断としての Automotive SPICE

1998 年 ISO/IEC TR 15504 の発行に伴い，システム技術研究会において，プロセスアセスメントの研究部会を開始した。ヨーロッパにおいては，ISO/IEC 15504 に基づいた作業診断モデル Automotive SPICE[23]が開発され，ヨーロッパの自動車メーカによる自動車の部品調達にあたって，作業改善の状況を確認するための方法として参考にされてきた。Automotive SPICE は，国際規格を作成するための標準情報であるISO/IEC TR 15504 part5の試行の経験に基づいて追加提案したプロセスを含んでいる。Automotive SPICE では複数の参照モデルからの引用の手間を省くため，ISO/IEC 12207 を引用した独自の参照モデルを作成している。

4.2 システム工学モデル

システム工学では，入力，状態（処理），出力をシステムと定義する。複雑なシステムは，制御可能な単純なサブシステムに分割する。制御システムもシステムの一部であるため，制御システムがシステムへ影響を与える可能性がある。そのため，制御システムは制御対象に対して，システムの初期条件などの制約を明確化が重要である。

プロセスは，入力を出力に変換するものである。入力と出力を測定することが，プロセスの測定の重要な部分である。出力から入力を引いた部分がそのプロセスで加わったものである。ISO/IEC 15504 part5 では入力と出力の作業生産物はなるべく同じ程度例示するようにしている。これを入出力の対照性と呼ぶ。入出力の品質指標は生産品目の機能と規模によるため，改善のための測定とその値に基づく改善の中で制定していくとよい。

SEI の CMM は調達にあたって，優秀な技術者が Ada などの最新の技術を利用しても，納期が守れない原因を追究するための調査に始まっている。日本をはじめとする各国の開発体制を調査している。CMM では，ベストプラクティスという「やっていてよかったこと」を体系的にまとめたものがモデルの基本要素である。

4.3 研究試作

最小セット OS は，研究試作の第二段階である。企業等における作業診断においては，量産段階の開発を対象にすることはあるが，研究試作の段階を診断した結果の報告はあまり知られていない。研究試作段階における作業方法としては，アジャイルが似たやり方であると考えられる。現在，ISO/IEC JTC1 SC7 においてアジャイルの工業標準化の可能性について Study Group が 2 年目に入っている。研究試作を標準化することは，人の能力に応じた作業定義の必要性の議論のきっかけとしたい。

4.4 追加定義

現在審議中の ISO/IEC TR 15504 part9 Target profile では，診断対象に応じて，対象となるプロセス（作業）を追加定義して診断することを検討している。ISO/IEC 15504 の試行を行ってきた際に，いくつかの視点が欠けていることを確認している。今回の作業においては，不足していると思われる事項を，追加定義しようとしている。情報交換の仕組みに関連して，「御用聞きプロセス」，「根回しプロセス」を検討している。既存のモデルにも人材管理プロセス定義はあるが，健康管理については十分でないため「顔色伺いプロセス」として追加を検討している。ISO/IEC 15504 Part5 の指標には，原価に関するものが少ないため，「原価計算プロセス」を対象定義した。

4.5 作業群

ISO/IEC 15504 は，CMM などの既存のモデルの共通部分を規定することを目的として統合化したモデルの作成を実施しようとしてきた。しかし，CMM などのモデルでは，プロジェクト単位，企業単位での診断を想定しており，現場での改善に対して必ずしも有効であることは明確にはなっていない。ISO/IEC 15504 は，個々の作業に対しても助言が可能なように，1つのプロセス定義に対しても診断可能な枠組みとして検討してきた。人材，費用の権限のない作業をプロジェクト管理の視点での診断は条件を満たさないことが指摘されている。

4.6 規格の適合

国際規格の適合は，ISO/IEC Directives[39]，ISO/IEC 17000 シリーズ[40]が発行されている。製品試験の場合には，試験結果の妥当性が試験手順に基づいている場合がある。特定の手順で試験をすれば再現性があれば，手順に意味がある。しかし，ソフトウェア開発のように，同じ手順を取っても，再現性が必ずしもないものもある。ISO/IEC 15504 では，繰り返し可能であることについて記述しているが，人の側面，製品の違いについては十分ではなく，人に関する規格，製品に関する規格との連動が求められている。現在，ISO/IEC JTC1 SC7 に Conformity Assessment に関するガイドの作成が提案されている。

4.7 文書化

検証用及び実装用のソースコード（コメントを含む），TOPPERS 関連仕様書，開発メモ[22]を含む関連文書，作業記録の4種類に分類している。作業記録は，異なる資金に基づく作業は，異なるメーリングリストに報告することにより，原価計算可能な記録として利用することを検討している。また，できるだけ多くの文書を TRAC に登録することによって，課題の明確化を図る予定である。自己改善できる人だけが従事している作業では，作業の指示はなく，事前に作業を定義しない。記録から，やっていてよかったことを副産物として整理する予定である。

5 まとめと今後の課題

従来，研究試作は作業診断の対象外においている場合があった。今回の設計作業にあたっては，要素技術の検討，診断の仕組みの課題，実際の作業への適用への鍵を検討した。研究試作であるか，量産試作であるかは要素技術の評価が済んでいるかどうかの違いであり，ETSS の仕組みによって能力に応じた作業判定を行うことにより，研究試作への適用が可能であると考えられる。

量産試作などにおいても，作業者の能力に応じた作業の枠組みに対応した診断は，ハードウェアとソフトウェアを平行開発する作業における有効性を検討したい。診断を実施する側の能力判定を ETSS 及び能力ガイドに基づいて行うことが今後の課題である。

成果の最初の普及は技術者研修を想定しており，多くの製品試作の初期段階に必要な機能をどの程度網羅しているかが技術的な課題である。

謝辞

本稿は，システム技術研究会 SPA 研究部会の講師の方々，情報処理学会情報規格調査会 SC7WG10 委員の皆様，二本規格協会情報技術標準化研究センター SPI-WG の皆様，IPA/SEC SPI-WG の皆様を始め多くの方々の指導をいただいたことに感謝いたします。

参考文献

[1] TOPPERS/JSP カーネル Release 1.4.2, TOPPERS

プロジェクト, http://www.toppers.jp/jsp-kernel.html, 2005
[2] μITRON4.0 仕様（Ver. 4.02.00; 日本語版）, (社)TRON 協会, http://www.ertl.jp/ ITRON/SPEC/mitron4-j.html, 2004
[3] M16C/62 グループユーザーズマニュアル, Renesas , 2001
[4] 斉藤直希, 竹内良輔, TOPPERS/JSP カーネルユーザズマニュアル M16C/M32C ターゲット依存部（M16c.txt/ M32C.txt）, TOPPERS, 2004
[5] IEC 61882:2001 Hazard and operability studies (HAZOP studies) - Application guide
[6] ISO 17356-3:2005 Road vehicles -- Open interface for embedded automotive applications – Part 3: OSEK/VDX Operating System (OS)
[7] 組込みシステム開発事例集, 産業技術連携推進会議 情報・電子部会 組込み技術研究会, 工業調査会, 2006
[8] ISO/IEC 19501:2005 Information technology -- Open Distributed Processing -- Unified Modeling Language (UML) Version 1.4.2
[9] IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
[10] ISO 9000:2005 Quality management systems -- Fundamentals and vocabulary
[11] ISO TS16949:2009 Quality management systems -- Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations
[12] IEC 60812:2006 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
[13] IEC 61025:2006 Fault tree analysis (FTA)
[14] 堀武司, 堤大祐, 小川清, 斉藤直希, 公設試験研究機関における組込みオープンソースソフトウェア TOPPERS による企業向け研修について,情報処理学会全国大会, 2005
[15] 小川清, 斉藤直希, 吉川直邦, 伊藤正樹, 後田直樹, 藩建華,リアルタイム組込みソフトウェアの用語の木,実時間処理ワークショップ（RTP2003）, IPSJ, 2003
[16] ISO/IEC 15504-2: information technology - process assessment, 2003
[17] 組込み開発者におくる MISRA-C―組込みプログラミングの高信頼化ガイド, MISRA-C 研究会, 日本規格協会, 2004
[18] 組込み開発者におくる MISRA‐C:2004―C 言語利用の高信頼化ガイド, SESSAME/MISRA‐C 研究会, 日本規格協会, 2006
[19] 吉川直邦, 坪井泰樹, 斉藤直希, 小川 清, MISRA-C: 1998 と MISRA-C:2004 の C90, C99 との検討,情報処理学会全国大会, 2005
[20] ISO/IEC 9899:1999,Cor 1:2001,Cor 2:2004, Programming languages C, ISO, 2004
[21] 斉藤直希, 渡部謹二, 小川 清, 大澤史郁, 大槻直哉, TOPPERS/JSP の M16C/M32C での移植, 情報処理学会組込みシステム研究会, 2006. 6
[22] 今井和彦, TOPPERS プロジェクト/JSP カーネル SH1 版・設計メモ, http://www.mit.pref.miyagi.jp/embedded/TOPPERS/index.html, 2001.9
[23] Automotive SPICE, http://www.automotivespice.com/
[24] Ogawa Kiyoshi, Fujino Kiichi, Trial Report from Northern Pacific Asia- Problems and Proposes for the phase 2 trial of software process assessment in Japan, SPICE97, IEEE, Walnut Creek, June, 1997
[25] Ogawa Kiyoshi, A practical assessment model for small enterprises in Japan, 第2回世界ソフトウェア品質会議, Yokohama, Aug, 2000
[26] 斉藤直希, 小川 清, 水口大知, 菊池達也, 大西秀一, 長谷部浩二, 堀 武司, コンポーネントソフトウェアに対するハザード分析手法の検討, 第五回システム検証の科学技術シンポジウム(SSV 2008) , 2008
[27] 小川 清, 斉藤直希, 堀 武司, 水口大知, 吉岡律夫, 森川聡久, 服部博行, ソフトウェア開発における安全分析, 形式手法, 工業標準に焦点をあてた安全関連スキルと教育訓練, 第五回システム検証の科学技術シンポジウム(SSV 2008) , 2008
[28] 堀 武司, 岡村真吾, 服部智幸, 斉藤直希, 小川清, 機能安全対応組込みソフトウェア開発における B メソッド導入の試み, 第五回システム検証の科学技術シンポジウム(SSV 2008) , 2008
[29] ETSS, 組込みスキルスタンダード, https://sec.ipa.go.jp/std/eb.php, 2006
[30] ISO/IEC 9126-1:2001 Software engineering -- Product quality -- Part 1: Quality model
[31] ISO/IEC 25000:2005 Software Engineering -- Software product Quality Requirements and Evaluation(SQuaRE) -- Guide to SQuaRE
[32] CMM, Software Engineering Institute(SEI)
[33] CMMI. SEI, www.sei.cmu.edu
[34] Introduction to the Personal Software Process(sm) , Watts S. Humphrey, 1996
[35] Introduction to the Team Software Process(sm) , Watts S. Humphrey, 1999
[36] ISO/IEC 24773 Software Engineering - Certification of software engineering professionals - Comparison framework.
[37] ISO/IEC 12207 software life cycle process
[38] ISO/IEC 15288 system life cycle process
[39] ISO/IEC Directives
[40] ISO/IEC 17000 シリーズ