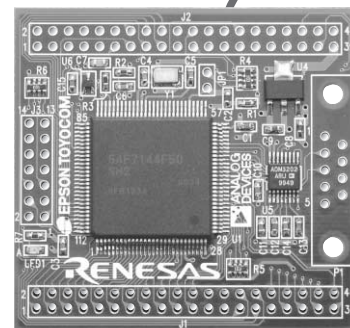


TOPPERS/OSEKカーネルにおける検証の実際

OS検証の自動実行による信頼性向上の手法

森川 聡久/杉本 明加



本誌 2006 年 8 月号特集記事では、OSEK/VDX OS 仕様^{注1}に準拠した TOPPERS/OSEK カーネルを SH-2 付録基板(本誌 2006 年 6 月号付録)に移植し、その移植手順について紹介しました。移植した OS を実用的に使用するためには、OS が正しく動作するか検証する必要があります。従来の手法では、この検証に工数がかかるため、OS 移植の問題点の一つとなっています。

今回は、移植した TOPPERS/OSEK カーネルについての適合試験と性能評価、それらを自動で実施するための自動実行環境について紹介します。今回の対象は TOPPERS/OSEK カーネルですが、OS 検証の自動実行についての手法は、ほかの OS にも応用できる考えでしょう。

1 適合試験仕様の作成

適合試験とは何か

適合試験とは、開発した OS が仕様書どおりに動作するかを確認することをいいます。

OSEK/VDX には、MODISTARC(Methods and tools for the validation of OSEK/VDX based distributed architectures)という適合試験仕様があり、MODISTARC プロジェクトより公開されています。

試験にあたっては、満たすべき仕様が重要になるので、まずは MODISTARC 仕様を参考にした適合試験について説明します。

表 1 MODISTARC 仕様書一覧(2006 年 7 月 31 日現在)

MODISTARC 仕様書名称	概要	OSEK/VDX の対応仕様書
OSEK/VDX Conformance Testing Methodology Version 2.0	MODISTARC の概要について書かれたもの	
OSEK/VDX Operating System Test Plan Version 2.0	OS 仕様よりテストすべき機能項目を洗い出し整理したもの	OSEK/VDX Operating System Version 2.0 revision 1
OSEK/VDX Operating System Test Procedure Version 2.0	OS テスト計画仕様書を元に作成したテスト・シーケンス仕様	
OSEK/VDX Communication Test Plan Version 2.0	COM 仕様よりテストすべき機能項目を洗い出し整理したもの	OSEK/VDX Communication Version 2.1 revision 1
OSEK/VDX Communication Test Procedure Version 2.0	COM のテストを行うためのテスト環境仕様。通信のテストを行うため、特別な環境となっている	
OSEK/VDX Communication Test Suites Version 2.0	COM テスト計画仕様書を元に作成したテスト・シーケンス仕様	OSEK Network Management Version 2.50
OSEK/VDX Network Management Test Plan Version 2.0	NM 仕様よりテストすべき機能項目を洗い出し整理したもの	
OSEK/VDX Network Management Test Procedure 2.0	NM のテストを行うためのテスト環境仕様。ネットワーク管理のテストを行うため、特別な環境となっている	
OSEK/VDX direct Network Management Test Suites 2.0	NM テスト計画仕様書を元に作成したテスト・シーケンス仕様。管理方法の異なる 2 種類	
OSEK/VDX indirect Network Management Test Suites 2.0	(direct, indirect) の NM が存在するため、仕様書も二つに分けてあるようだ	

注 1 : OSEK/VDX(Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug/ Vehicle Distributed eXecutive)とは、欧州の自動車産業が中心となって策定した、自動車向き OS の標準仕様。おもに、OS 仕様、COM(通信)仕様、NM(ネットワーク管理)仕様がある。

OSEK/VDX における適合試験仕様 MODISTARC の概要

MODISTARC の仕様書は、OSEK/VDX の Web サイト (<http://www.osek-vdx.org/>) より、「MODISTARC」 「Specifications」とたどって、だれでもダウンロードすることができます。

現在公開されている仕様書とその概要を表 1(p.163)にまとめます。MODISTARC 仕様は OSEK/VDX OS 仕様、OSEK/VDX COM(通信)仕様、OSEK/VDX NM(ネットワーク管理)仕様の 3 種類について策定されています。

また、MODISTARC 仕様のテスト・シーケンス作成の流れは、図 1 のようになっています。(1)適合仕様の抽出では、何についてテストすべきかを仕様書から洗い出します。(2)テスト・ケースの作成では、抽出した適合仕様を元に整理し、最適なテスト・ケースを作成します。ここでは Test Plan 仕様書にて説明されています。

続いて、(3)テスト・シーケンスの作成では、作成したテスト・ケースを組み合わせ、最適なテスト・シーケンスを作成します。OSEK/VDX OS 仕様に関しては Test Procedure 仕様書で、OSEK/VDX COM 仕様と OSEK/VDX NM 仕様に関しては Test Suites 仕様書で説明されています。さらに、(4)テスト実施では、テストを実施するためのテスト環境に関して、Test Procedure 仕様書にて説明されています。

このように、MODISTARC 仕様書では、テスト・シーケンスが完成するまでの流れがていねいに説明されています。そのため、使用する OS のバージョンが一致する場合は、最後の完成したテスト・シーケンスのみを参照するだけでかまいません。

今回はカーネルの適合試験を行うので、以降は OSEK/VDX OS 仕様の MODISTARC 仕様について詳細を解説します。図 2 は、OSEK/VDX OS 仕様の MODISTARC 仕様に基づいたテスト・シーケンスの作成の流れについて、割り込み処理に関するテストを例に挙げています。

適合仕様の抽出

仕様書からテストすべき項目である適合仕様を洗い出します。たとえば、

- 割り込みと OS はタスクよりも優先度が高いこと
 - タスクの優先度は 8 レベル以上あること
- といったものです。

適合仕様はかなりの数に上るので、機能単位で洗い出すほうがよいでしょう。MODISTARC 仕様書では、次のような機能分けを行い、それぞれについて 4 ~ 18 項目挙げています。

- 実装パラメータ
- タスク管理
- 割り込み処理
- イベント・メカニズム
- リソース管理
- アラーム
- そのほか(エラー・ハンドリング、フック・ルーチン、OS 実行制御)

図 2(a) は割り込み処理に関する適合仕様の抜粋です。割り込み処理に関する説明文と、OS の仕様書から抽出したテストすべき内容を整理した表が記載されています。「OS は割り込みを許可・禁止できるサービスを提供すること」、「それらのサービスは割り込みサービス・ルーチン内でも使用可能であること」、「カテゴリ 2 割り込み中は、OS のサービスが制限されること」が挙げられています。表には関連する仕様書の記述箇所、さらにその仕様を満たすための、テスト時の OS 設定値も記述されています。

OS 設定値を表 2 にまとめます。この 3 項目についてそれぞれの設定値を選択する必要があります。

テスト・ケースの作成

次にテスト・ケースを作成します。ここでのテスト・ケースとは、テストすべき具体的な小項目に相当します。たとえば、

- 不正なタスク ID でタスク起動要求 `ActivateTask()` を呼び出した結果、`E_OS_ID` エラーが返る
- ノンプリエンティブ・タスクが `ActivateTask()` 要求した場合、処理は成功し、起動されたタスクは Ready 状態になる
- プリエンティブ・タスクが優先度の高いタスクを `ActivateTask()` 要求した場合、処理は成功し、起動されたタスク

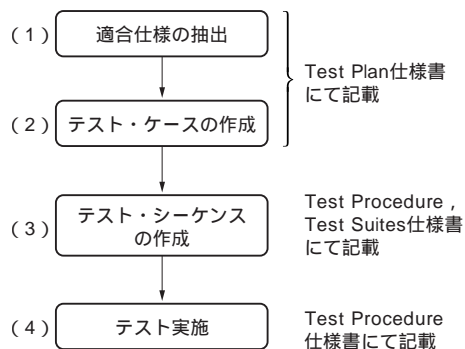


図 1 テスト・シーケンス作成の流れ

表 2 テスト時の OS 設定値

OS 設定項目	設定値
スケジューリング・ポリシー	n : Non Preemptive m : Mixed Preemptive f : Full Preemptive
パフォーマンス・クラス	B1 : BCC1 B2 : BCC2 E1 : ECC1 E2 : ECC2
システム・サービスのエラー・チェック・レベル	s : Standard Status (警告状態を正常状態として継続実行) e : Extended Status (警告状態の場合エラーの詳細を返す)