Empowered by Innovation NEC

リアルタイムOSの高信頼性検証
（分析／設計編）

日本電気通信システム株式会社
大黒 ゆき子　長山 卓也　山下 映　内山 美佐子

独立行政法人 宇宙航空研究開発機構
石濱 直樹

目次

1. はじめに
2. リアルタイムOSの高信頼性検証ガイドラインの必要性
3. 分析と設計のガイドライン（動的検証用）の策定
4. 高信頼性検証内容の導出
5. 分析のための活動
6. 設計のための活動
7. ガイドラインの利用
8. おわりに

補足資料-A　分析ポイントの例
補足資料-B　テストケース作成ポイントの例
補足資料-C　入力値指標の例

1. はじめに

組込みソフトウェアは、高機能化・大規模化しており、リアルタイムOSの需要は、より高まっている。
また、宇宙機システムを含む、多くの組込みソフトウェアには、高い信頼性や安全性が求められる 。

このような背景から、高信頼性を確保したリアルタイムOSが求められている。

我々は、リアルタイムOSの高信頼性を確保するための検証ガイドラインの検討を行っている。

今回は、リアルタイムOS検証ガイドラインの必要性、ガイドライン策定に係る活動、およびガイドラインの利用効果を紹介する。

イメージ画像　Courtesy of JAXA

2. リアルタイムOSの高信頼性検証ガイドラインの必要性

ソフトウェア開発ガイドラインは存在するが、リアルタイムOSに特化したガイドラインが存在しない

- リアルタイムOSは、アプリケーションとは異なる下記の特徴をもつ。
  そのため、リアルタイムOSに特化した検証ガイドラインが必要である。

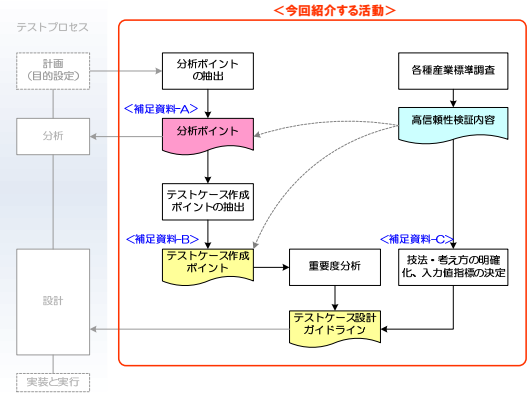
リアルタイムOSの主な特徴（リアルタイムOSの特異性）
- ハードウェアに依存する部分を持つ
- 複数のタスクを管理する機能を持つ
- 時間を管理する機能を持つ
- 割込みを管理する機能を持つ
  ：

リアルタイムOSに特化した、「分析と設計のガイドライン（動的検証用）」の策定活動を、以降に紹介する。

リアルタイムOSの検証ガイドライン

計画とコントロールのガイドライン | **分析と設計のガイドライン** | 実装と実行のガイドライン | 終了基準とレポートのガイドライン

3. 分析と設計のガイドライン（動的検証用）の策定



4. 高信頼性検証内容の導出

産業標準から高信頼性検証内容を導出

- 信頼性・安全性が重視される**産業分野の標準を調査**し、高信頼性検証に適用するテスト技法やテスト基準を導きだし、**高信頼性検証内容**を策定した。

＜ 産業標準 ＞

分類	標準
産業一般	JIS C 0508(IEC61508-7)
医療機器	General Principles of Software Validation; Final Guidance for Industry and FDA Staff
原子力発電所	IEC880(IEC60880) Edition1
鉄道	EC 6229 Edition 1
軍事機器	DEF STAN 00-42(PART2) Issue 1
民間航空機	RTCADO-178B

＜ 高信頼性検証内容 ＞

テスト項目	詳細テスト項目
要求事項	外部要求事項のテスト
	内部要求事項のテスト
入力域	代表値のテスト／同値分割
	境界値分析／異常入力域のテスト／ロバストネステスト／極端な値のテスト／クラッシュテスト
システム構造	データ結合および制御結合の網羅テスト
	状態遷移テスト
	ソフトウェアインタフェーステスト
	ハードウェア・ソフトウェアインタフェーステスト
	ハードウェア障害対応テスト
モジュール内構造	MC/DCテスト
	条件網羅テスト
	命令網羅テスト
	ループテスト（最小・最大・中間回数）
	データフローパステスト
メモリ関連	メモリ割り当てテスト
	メモリ参照テスト
割込み・タイミング・資源	割込みシーケンスの最大組み合わせテスト
	資源テスト
特殊な観点	エラー推測テスト

※JAXA「高信頼性模証要求の検討結果」より。

5. 分析のための活動

分析ポイントの抽出

- 検証の目的を元に分析ポイントを抽出し、明文化した。[補足資料-A参照]
  分析ポイントの抽出にあたっては、特に以下に留意した。
  - ✓ **多角的な観点**
  - ✓ **リアルタイムOSの特性を考慮**

＜分析ポイント（第一階層）＞

	単体テスト	結合テスト	システムテスト
機能	詳細設計	基本設計 インタフェース 割込み 初期設定 異常処理 状態	システム要求 割込み リソース 性能 ディスパッチ 負荷 競合 異常処理
構造	計算式 分岐条件 ループ 比較 命令	関数コール 関数ポインタ	
データ	入出力パラメータ ポインタ グローバルデータ	アクセサメモリ ポインタ グローバルデータ	入出力パラメータ
特殊な観点	コーディング規約 異常データ 開発環境	例外処理 BSP	資源 メモリ破壊

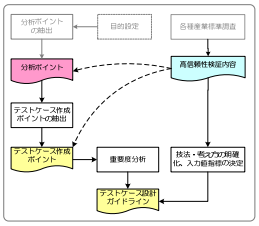
6. 設計のための活動

テストケース作成ポイントの抽出

- 分析ポイントから**テストケースの作成ポイント**を抽出し、明文化した。[補足資料-B参照]

重要度分析

- テスト戦略に従って取捨選択が出来るようにポイントの**重要度分析**を行った。



技法・考え方の明確化、入力値指標の決定

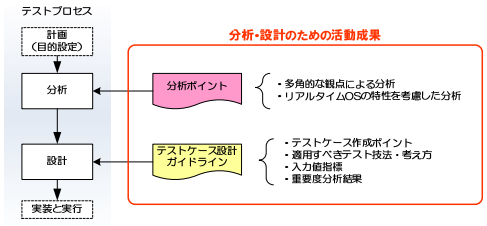
- テストケース作成のばらつき低減や、テストパターンの漏れ防止、及びテスト設計の容易化を目的に、**技法や考え方、入力値指標**を明文化した。[補足資料-C参照]

テストケース設計ガイドラインの策定

7. ガイドラインの利用

テストケース設計ガイドライン等の利用により、リアルタイムOSの高信頼性検証での分析、設計において、以下のような効果が得られる。

- リアルタイムOSに最適な高信頼性検証の実現
- 分析・設計の属人性低減と容易化
- テスト戦略に適合したテストケースの作成



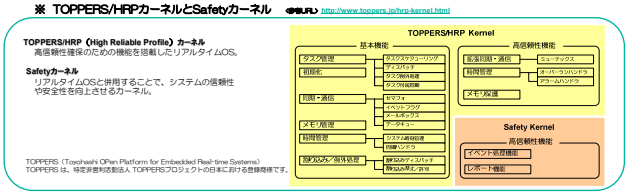
8. おわりに

今回、リアルタイムOSの高信頼性検証のガイドライン策定に関する活動の一部として、分析と設計に焦点を当てた紹介を行った。

なお、実在するリアルタイムOS（※下記）を検証対象として、ガイドラインの有用性や妥当性を実証する活動も行っている。

これらは現在進行中であり、今後も「**リアルタイムOSの高信頼性検証ガイドライン策定**」を目標に、活動を継続する。

※ TOPPERS/HRPカーネルとSafetyカーネル　URL: http://www.toppers.jp/hrp-kernel.html



Empowered by Innovation

NEC

NEC通信システム

補足資料-A　分析ポイントの例

＜分析ポイント例＞

（３） 割り込み／例外

RTOS では管理対象の割り込み（以降、例外も含む）が発生すると、定義した割り込みハンドラを起動させる。RTOS は、割り込みを管理することにより、現在、通常処理のコンテキストであるか、割り込みのコンテキストであるかを把握する。また、管理対象の全ての割り込みにおいて、割り込みが発生した場合には、コンテキスト退避／復帰などの適切な処理を行う。

割り込み／例外の分析ポイントを表 3-7に示す。

表 3-7　割り込み／例外の分析ポイント

割り込み／例外の分析ポイント		
コンテキスト範囲	CPU	CPU 内の PC（プログラムカウンタ）、SP（スタックポインタ）、レジスタや浮動小数点レジスタ、メモリ等のコンテキスト切り替え時の保存すべきコンテキストには何があるか。
	メモリ	
コンテキスト退避／復帰		割り込み／例外発生時のコンテキストの退避／復帰の仕組みがどのようになっているか。
割り込み禁止／許可		割り込み禁止／許可の仕組みがどのようになっているか。
		割り込み禁止と許可の間の時間が長くなるのはどのような場合か。
		CPU の特性上で問題となる部分（ＣＰＵハザード等）はないか（例：割り込み許可命令受付後、ある一定クロック数経過後にしか割り込みを受け付けない等）。
多重割り込み		何重の割り込み／例外まで管理を行っているか。
		割り込みが発生している場合の割り込み禁止／許可の仕組みがどのようになっているか。
複数割り込み		同時に割り込みが発生した場合の挙動はどのようになっているか。

補足資料-B　テストケース作成ポイントの例

<テストケース作成ポイント例>

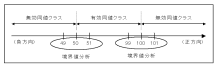
No.	大項目	小項目	テストケース抽出ポイント	高信頼性検証要求の検討結果 (*3)	
				詳細テスト項目	テスト項目
1	機能	詳細設計	詳細設計書を基に各関数に求められる機能が実装されていることを確認する。	内部要求事項のテスト	要求事項のテスト
2	構造	計算式	計算式から入力値および得られる結果を同値に分割し、同値内の代表値を使用して確認する。	代表値のテスト／同値分割	入力域のテスト
3			計算式から入力値および得られる結果の取り得る値の範囲をチェックし、境界値として最大／最小値及び最大値±1／最小値±1 を入力して動作に問題ないかを確認する。	境界値分析	
4			計算式の開値（計算結果が連続でなくなる点）を入力して動作に問題ないかを確認する。	計算式の開値テスト	
5			開値の前後の値をテストケースとして挙げる。計算式の結果、桁あふれや０になる場合に起因する例外を入力して動作に問題ないかを確認する。	エラー推測テスト	
6			No. 2~5 の計算式についてのテストケースを実施した結果、０除算とならないことを確認する。		モジュール内構造のテスト
7		条件分岐	全ての分岐条件が正しいかを確認する。	命令網羅テスト	
8			条件項を同値に分割し、同値内の代表値を入力して動作に問題ないかを確認する。	MC/DC テスト or 条件網羅 (C1) or 複合条件網羅 (C2)	
9			条件項 (*1) の同値クラスの境界値をチェックし、境界値として最大／最小値及び最大値±1／最小値±1 を入力して動作に問題ないかを確認する。		
10			MC/DC を実施する場合、各条件項のとりうる結果 (TRUE/FALSE) を少なくとも一度は実行し、各々の条件項の TRUE/FALSE と判定結果 (TRUE/FALSE) の組み合わせを使用して確認する。	MC/DC テスト	
11			条件網羅 (C1) を実施する場合、各条件のとりうる結果 (TRUE/FALSE) を少なくとも一度は実行するように確認する。	条件網羅 (C1)	
12			複合条件網羅 (C2) を実施する場合、複数の条件で各条件のとりうる結果 (TRUE/FALSE) の組み合わせを全て実行するように確認する。	複合条件網羅 (C2)	

補足資料-C　入力値指標の例

●境界値分析

境界値分析により、変数 "x" の取り得る値の範囲について、その最小境界値、最大境界値に対して、以下の試験値を設定する。それぞれの値は、境界値を含む／含まない場合で、意味付けが変わるが、有効同値クラスと無効同値クラスの切り替わる値の確認は行える。

試験値	境界値を含む	境界値を含まない
最小境界値－1	無効同値クラス	無効同値クラス
最小境界値	有効同値クラス	無効同値クラス
最小境界値＋1	有効同値クラス	有効同値クラス
最大境界値－1	有効同値クラス	有効同値クラス
最大境界値	有効同値クラス	無効同値クラス
最大境界値＋1	無効同値クラス	無効同値クラス

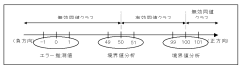


●　極端な値

極端な値として、試験対象となる変数の型の取り得る最大、および最小値に対する境界値を試験値として設定する。試験値の性質上、最大値＋1　および、最小値－1　は無効とする。この試験値によるテストは、入力パラメータに対する動作確認を想定している。そのため、外部変数等のシステムが保持するデータに対するテストに本試験値は適用せず、サービスコールの入力に対してのみ適用する。

●エラー推測

符号が変わる境界値については、エラー推測値として必ず試験を実施する。



エラー推測値とて（－1，0，1）を設定しているが、変数が符号無し（unsigned）の場合、エラー推測値は（0，1）となる。