

次世代車載システム向け RTOS 要求仕様書

Ver.2.0.0

2013/1/22

Copyright (C) 2011-2013 by Center for Embedded Computing Systems

Graduate School of Information Science, Nagoya Univ., JAPAN

Copyright (C) 2011-2013 by FUJISOFT INCORPORATED, JAPAN

Copyright (C) 2011-2013 by FUJITSU VLSI LIMITED, JAPAN

Copyright (C) 2011-2013 by NEC Communication Systems, Ltd., JAPAN

Copyright (C) 2011-2013 by Panasonic Advanced Technology Development Co., Ltd., JAPAN

Copyright (C) 2011-2013 by Renesas Electronics Corporation, JAPAN

Copyright (C) 2011-2013 by Sunny Giken Inc., JAPAN

Copyright (C) 2011-2013 by TOSHIBA CORPORATION, JAPAN

Copyright (C) 2011-2013 by Witz Corporation, JAPAN

上記著作権者は、以下の (1)~(3)の条件を満たす場合に限り、本ドキュメント（本ドキュメントを改変したものを含む、以下同じ）を使用・複製・改変・再配布（以下、利用と呼ぶ）することを無償で許諾する。

- (1) 本ドキュメントを利用する場合には、上記の著作権表示、この利用条件および下記の無保証規定が、そのままの形でドキュメント中に含まれていること。
- (2) 本ドキュメントを改変する場合には、ドキュメントを改変した旨の記述を、改変後のドキュメント中に含めること。ただし、改変後のドキュメントが、TOPPERS プロジェクト指定の開発成果物である場合には、この限りではない。
- (3) 本ドキュメントの利用により直接的または間接的に生じるいかなる損害からも、上記著作権者および TOPPERS プロジェクトを免責すること。また、本ドキュメントのユーザまたはエンドユーザからのいかなる理由に基づく請求からも、上記著作権者および TOPPERS プロジェクトを免責すること。

本ドキュメントは、無保証で提供されているものである。上記著作権者および TOPPERS プロジェクトは、本ドキュメントに関して、特定の使用目的に対する適合性も含めて、いかなる保証も行わない。また、本ドキュメントの利用により直接的または間接的に生じたいかなる損害に関しても、その責任を負わない。

<目次>

1. 概要	1
1.1 本文書の目的	1
1.2 関連文書	1
1.3 凡例	1
2. 要件	2
2.1 AUTOSAR OS 仕様との関連	2
2.1.1 【REQ001】 ベースとする仕様	2
2.1.2 【REQ002】 ベース仕様の明確化	2
2.1.3 【REQ003】 ベース仕様の修正	2
2.2 保護機能	3
2.2.1 【REQ004】 保護機能における機能レベルの設定	3
2.2.2 【REQ005】 メモリ保護機能における実装依存規定の排除	3
2.2.3 【REQ006】 メモリ保護機能のコンフィギュレーションの標準化	3
2.2.4 【REQ007】 非信頼 OS アプリケーションに対する制限の緩和	3
2.3 マルチコア拡張	4
2.3.1 【REQ008】 OS のマルチコア対応	4
2.3.2 【REQ009】 マルチコア対応 OS のリアルタイム性能	4
2.3.3 【REQ010】 マルチコア対応 OS における OS オブジェクトのコア割付け	4
2.3.4 【REQ011】 マルチコア対応 OS におけるタスクオブジェクト	4
2.3.5 【REQ012】 マルチコア対応 OS におけるリソースオブジェクト	5
2.3.6 【REQ013】 マルチコア対応 OS におけるブロッキングによる排他制御機構	5
2.3.7 【REQ014】 マルチコア対応 OS におけるカウンタ，アラーム，スケジュールテーブル	5
2.3.8 【REQ015】 マルチコア対応 OS におけるフックルーチン	5
2.3.9 【REQ016】 マルチコア対応 OS におけるコア間通信	6
2.3.10 【REQ017】 マルチコア対応 OS における OS の起動，終了	6
2.3.11 【REQ018】 マルチコア対応 OS における OS アプリケーション	6
2.4 その他	7
2.4.1 【REQ019】 OS によるメモリの活用	7
変更履歴	8

1. 概要

1.1 本文書の目的

本文書は「次世代車載システム向け RTOS 外部仕様書」で規定される OS 機能仕様に対する，基本的な要求仕様を規定する。ただし，次世代車載システム向け RTOS 外部仕様書において，マルチコアに対する仕様は，現在検討中であるため，今後本仕様を変更する可能性がある。

1.2 関連文書

文書名	バージョン
次世代車載システム向け RTOS 外部仕様書	Ver.2.0.0
次世代車載システム向け RTOS 用語集	Ver.2.0.0

1.3 凡例

本仕様書では各要件に対して以下に示す要件番号を付加して管理を行う。

凡例	内容
【REQxxx】	OS 機能に対する要件番号．本仕様書において規定．
【NOSxxx】	OS 仕様のうち，NCES にて新規に規定した仕様に対する番号．「次世代車載システム向け RTOS 外部仕様書」において規定された番号を参照している．

2. 要件

2.1 AUTOSAR OS 仕様との関連

2.1.1 【REQ001】ベースとする仕様

AUTOSAR OS 仕様をベースとすること.

要求の理由

車載システムにおいて標準で使用されてきた OSEK/VDX と、その上位互換である AUTOSAR OS 上で構築されたソフトウェア資産の継承を容易にするため.

2.1.2 【REQ002】ベース仕様の明確化

AUTOSAR OS 仕様において曖昧な仕様を、明確に規定すること.

要求の理由

AUTOSAR OS 仕様には、仕様の解釈が多様になされる恐れがある仕様規定が存在する. このような仕様を明確に規定することによって、アプリケーションプログラムの移植性を向上させる.

2.1.3 【REQ003】ベース仕様の修正

AUTOSAR OS 仕様に不都合がある場合には、必要な修正を加えること.

要求の理由

AUTOSAR OS 仕様には、規定の矛盾や性能低下が懸念されるなどの不都合な規定が存在する. このような仕様の見直しを全体的に行い、必要に応じて修正を加えて仕様の完成度を高める.

2.2 保護機能

2.2.1 【REQ004】保護機能における機能レベルの設定

AUTOSAR OS 仕様の保護機能に対して機能レベルを設定することで、オーバーヘッドの小さな実装を可能にすること。

要求の理由

AUTOSAR OS 仕様の各種の保護機能に関して、オーバーヘッドの大幅な増加が見込まれるという懸念がある。アプリケーションプログラムからの機能要求とハードウェア性能との兼ね合いから、規定の保護機能をサブセット化してオーバーヘッドを軽減するような実装を可能とする。

2.2.2 【REQ005】メモリ保護機能における実装依存規定の排除

AUTOSAR OS 仕様のメモリ保護機能に関する実装依存規定を減らすこと。

要求の理由

メモリ保護を実現するハードウェアの持つ機能が多種多様であることから、AUTOSAR OS 仕様ではメモリ保護機能として満たすべき機能規定の多くがオプション（“The Operating System may …”という記述）となっている。これらを OS に搭載すべきか否かを明確に規定することで異なる OS 実装の間での搭載機能の違いが生ずることを防ぐ。

2.2.3 【REQ006】メモリ保護機能のコンフィギュレーションの標準化

プログラムのコード領域やデータ領域に対するメモリ保護のコンフィギュレーションが、ターゲットプロセッサや開発環境に依存せずに行えること。

要求の理由

ターゲットプロセッサをサポートする開発環境（コンパイラ、リンカ）の提供する機能が多様であることから、AUTOSAR OS 仕様ではメモリ保護のコンフィギュレーション仕様を標準化していない。これらの仕様を標準化することで、異なるターゲットプロセッサ間でのアプリケーションプログラムの移植性を向上させる。

2.2.4 【REQ007】非信頼 OS アプリケーションに対する制限の緩和

非信頼 OS アプリケーションから指定した周辺デバイスへアクセスを許可する機能を持つこと。

要求の理由

AUTOSAR OS 仕様では、信頼 OS アプリケーションのみが周辺デバイスへのアクセスすることを許しており、非信頼 OS アプリケーションから周辺デバイスを利用する場合は信頼 OS アプリケーションに処理を依頼する必要があるため、オーバーヘッドの著しい増加が見込まれる。保護が不要な周辺デバイスは非信頼 OS アプリケーションからのアクセスを許すことで、オーバーヘッドの軽減を図る。

2.3 マルチコア拡張

2.3.1 【REQ008】 OS のマルチコア対応

複数のコアを 1 つの OS で制御し、1 つのコンフィギュレーション記述によってコンフィギュレーションができること。

要求の理由

マルチコアシステムを構成する複数のコアの間で、ユーザがアプリケーションプログラムを任意に配置し、それらのプログラムが連携動作できなければならない。アプリケーションプログラム配置におけるユーザの利便性のため、コンフィギュレーションファイルを一本化する。アプリケーションプログラムの連携動作のため、各コアにおいて同一の OS を動作させてアプリケーションの実行制御を行う。

2.3.2 【REQ009】 マルチコア対応 OS のリアルタイム性能

車載制御システムに要求されるリアルタイム性を満たすこと。具体的には、OS 処理時間の上限を予測できること。また、割込み応答時間の最大値をコア数に依らずに保証できること。

要求の理由

システム全体のリアルタイム性を満たすためには、アプリケーションプログラムを構成するタスク、ISR のリアルタイム性を満たす必要がある。そのためには、タスク、ISR の動作を司る OS 処理時間の上限が予測可能であることは必須の条件となる。

2.3.3 【REQ010】 マルチコア対応 OS における OS オブジェクトのコア割付け

OS オブジェクト（タスク、ISR、リソース、カウンタ、アラーム、スケジュールテーブル）は、マルチコアシステムを構成するいずれか 1 つのコアに静的に割り付けること。タスクと ISR は、割り付けられたコアにて実行される。

要求の理由

タスクと ISR を実行するコアを固定することによって、OS 処理時間の上限が予測可能とするとともに、アプリケーションプログラムの振る舞いの再現性を確保する。

2.3.4 【REQ011】 マルチコア対応 OS におけるタスクオブジェクト

タスクに対する操作は割り付けられたコアに依存せずに行えること。具体的には、他のコアに割り付けられたタスクの起動やイベントのセットが行えること。

要求の理由

アプリケーションプログラムを構成するタスクが、マルチコアシステムを構成するコアにどのように分散して割付けられたとしても、タスク間の連携動作が可能でなければならないため。

2.3.5 【REQ012】 マルチコア対応 OS におけるリソースオブジェクト

異なるコアに割り付けられたタスクまたは ISR 間で排他制御するための機能を持つこと。また、排他制御にかかる最大時間を予測できること。

要求の理由

アプリケーションプログラムを構成するタスクと ISR が、マルチコアシステムを構成するコアにどのように分散して割付けられたとしてもタスク、ISR 間の排他制御を可能とするため。また、シングルコアにおけるリソースオブジェクトによる排他制御の前提（排他資源待ちにおいてブロッキングは生じない）との乖離をなくすため、ブロッキングではなくビジーウェイトで待ちを実現し、かつ、排他制御の処理の最大時間を予測可能とする。

2.3.6 【REQ013】 マルチコア対応 OS におけるブロッキングによる排他制御機構

異なるコアに割り付けられたタスク間で、ブロッキングを用いて排他制御する機能を持つこと。

要求の理由

要求【REQ12】の実現には、ビジーウェイトによるスループット低下の危険性が存在する。よって、ビジーウェイトによる排他制御機能に加えてブロッキングを用いた排他制御機構を提供し、両者を必要に応じて使い分けることを可能とする。

2.3.7 【REQ014】 マルチコア対応 OS におけるカウンタ、アラーム、スケジュールテーブル

異なるコアに割り付けられたタスクまたは ISR 間で、外界の任意のイベントの繰り返し回数に応じて同期動作するための機能を持つこと。

要求の理由

アプリケーションプログラムを構成するタスクと ISR が、マルチコアシステムを構成するコアにどのように分散して割付けられたとしても、カウンタによって駆動する同期動作を可能とする。

2.3.8 【REQ015】 マルチコア対応 OS におけるフックルーチン

フックルーチン（エラーフック、プロテクションフックは除く）は、コア毎に個別のルーチンが設定できること。

要求の理由

コアごとに接続される周辺デバイスが異なる場合、初期化、終了ルーチンはコアごとに別個の処理を記述する必要がある。また、各コアで実行されるタスクのスケジューリングをトレースする機能をコア個別に提供する。

2.3.9 【REQ016】 マルチコア対応 OS におけるコア間通信

タスクまたは ISR から、他のコアに対して割込みハンドラの起動を要求する機能を持つこと。

要求の理由

タスク操作（タスク起動やイベントセットのシステムサービス）による連携動作よりも、応答性の良いコア間の連携動作のための機能を提供するため。

2.3.10 【REQ017】 マルチコア対応 OS における OS の起動，終了

すべてのコアを同期して起動・終了することができること。

要求の理由

要求【REQ011】～【REQ014】から、各コア上で実行されるタスクは OS のシステムサービスを通じて他のコアのオブジェクトを操作する。そのため、マルチコアシステム中の一部のコアで、OS が動作していないという過渡的な状態を避けなければならない。

2.3.11 【REQ018】 マルチコア対応 OS における OS アプリケーション

OS アプリケーションが複数のコアにまたがることができること。具体的には、OS アプリケーションを構成する OS オブジェクトを複数のコアに割り付けることができること。

要求の理由

シングルコアで動作していた OS アプリケーションの性能向上のために、OS アプリケーションを構成するタスクを複数のコアに分散させ動作させるというコンフィギュレーションが考えられるため。また、マルチコアシステムに統合される OS アプリケーション間での保護を実現する必要があるため、OS アプリケーションを構成する OS オブジェクトのコアへの割付けに制限を加えない。

2.4 その他

2.4.1 【REQ019】 OS によるメモリの活用

ターゲットプロセッサに搭載されている各種のメモリの性質や容量に応じて、性能の向上を図ることのできる手段を提供すること。

要求の理由

リアルタイム性の観点では OS 処理時間の上限の予測可能性は必須としている。一方で、OS 処理性能（主に OS 処理時間の平均値）の向上を狙うことができるものの、実現性はターゲットに搭載されるメモリの容量、性質に依存する最適化が考えられる。これらに関しては、メモリに関するコンフィギュレーションの枠組みは規定しながらも、パラメータやその他の仕様規定に実装依存を許すことで、柔軟性を確保する。

変更履歴

Version	Date	Detail	Editor
1.0.0	2010/3/5	NCES 内部リリース	NCES
1.1.0	2010/12/1	TOPPERS 会員向け早期リリース	NCES
1.1.1	2011/12/28	ATK2 コンソーシアム向けリリース	NCES
1.1.2	2012/3/30	・ ファイル名から文書番号を削除 ・ コピーライトを記載 ・ 誤字, 脱字, 説明不足等を修正	NCES
2.0.0	2013/1/22	・ 要件と OS 仕様の対応を削除 ・ 一般向けリリース	NCES