文書番号：NGKA_REQ-01-301

NCES

次世代車載システム向け RTOS
要求仕様書

Ver.3.0.1

2014/3/12

名古屋大学大学院情報科学研究科附属 組込みシステム研究センター

＜目次＞

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．

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.3.0.0
次世代車載システム向け RTOS 用語集	Ver.3.0.0

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関して，オーバ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ナル（“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，オーバヘッドの軽減を図る．

2.3　マルチコア拡張

2.3.1　【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．

2.3.2　【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

スピンロックによるコア間の排他制御の実現には，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．

2.3.3　【REQ016】マルチコア対応 OS におけるコア間割込み

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．

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

シングルコア向けに開発した 1 つのアプリケーションを，性能向上のために複数のコアに跨って動作させる機能を持つこと．

要求の理由

AUTOSAR 仕様では，OSAP に所属する OS オブジェクトを，複数のコアに跨って割付けることができないが，シングルコアで動作していたアプリケーションの性能向上のために，OSAP 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．具体的な方法として，全く同じメモリ保護属性となる OSAP を複数のコアに定義可能とし，それぞれの OSAP にタスクを分散させる方法が考えられる．

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．

2.4.2　【REQ020】安全性の向上

OS は，可能な限り，エラーチェックや，異常検知を行い，アプリケーションをより安全に動作させることを可能にすること．

要求の理由

AUTOSAR OS 仕様だけでは, エラーチェックや, 異常検知に対する仕様が不足していると思われる．

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
3.0.0	2013/6/28	・AUTOSAR のマルチコア仕様に対応 ・NCES 独自のマルチコア拡張に対する要求仕様を削除	NCES
3.0.1	2014/3/12	コピーライト修正	NCES