

次世代車載システム向け RTOS 用語集

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
2. 用語集	2
変更履歴	7

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 要求仕様書」、「次世代車載システム向け RTOS ハードウェア要求仕様書」、「次世代車載システム向け RTOS 外部仕様書」で使用する，用語を定義する．

なお，次世代車載システム向け RTOS 外部仕様書の「主要概念」の節で，説明されている用語に関しては，本文書には記載しない．

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 要求仕様書	Ver.2.0.0
次世代車載システム向け RTOS ハードウェア要求仕様書	Ver.2.0.0
次世代車載システム向け RTOS 外部仕様書	Ver.2.0.0

2. 用語集

用語	定義
AUTOSAR	Automotive Open System Architecture の略語。 車載制御ソフトウェアの標準化、部品化を目的とした標準化団体。
OSEK/VDX	Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug / Vehicle Distributed eXecutive の略語。 欧州の自動車産業が中心となって設立されたプロジェクト。OS, ECU 間通信、ネットワーク管理について規定している。
ATK2	AuTomotive Kernel version 2 の略語。 NCES で開発した次世代車載システム向け RTOS の名称。TOPPERS プロジェクトよりオープンソースで公開する。
実装定義	1.2 節の関連文書では標準化せず、実装毎に規定すべき事項。 アプリケーションの中で、実装定義の事項に依存している部分は、移植性が保証されない。
実装依存	1.2 節の関連文書で定める機能仕様の中で、実装ないしはシステムの動作条件によって振る舞いが変わる事項。 アプリケーションの中で、実装依存の事項に依存している部分の振る舞いは、1.2 節の関連文書上では保証されない。
SCx	SC(スケーラビリティクラス)はユーザに必要な機能とターゲットの持つ機能によって OS 機能を定義した機能セットであり、SC1～SC4 がある。さらにマルチコア拡張の場合は、"-MC"を付加する。
OS オブジェクト	タスク、ISR、イベント、カウンタ、アラーム、スケジュールテーブル、リソース、信頼関数、OS アプリケーション固有のフックルーチン(SC3, SC4 のみ)、ミューテックス(参考仕様)。 特定の種別の OS オブジェクトを示す場合は、単に「～オブジェクト」と記載する(例：アラームオブジェクト)。
OS アプリケーション	OS オブジェクトの集合を OS アプリケーションと呼ぶ(SC3, SC4 のみ)。
信頼タスク	SC3, SC4 において、信頼 OS アプリケーションに所属するタスク。
非信頼タスク	SC3, SC4 において、非信頼 OS アプリケーションに所属するタスク。
信頼 C2ISR	SC3, SC4 において、信頼 OS アプリケーションに所属するカテゴリ 2ISR。
非信頼 C2ISR	SC3, SC4 において、非信頼 OS アプリケーションに所属するカテゴリ 2ISR。

用語	定義
信頼フック	SC3, SC4において、信頼 OS アプリケーションに所属する OS アプリケーション固有のスタートアップフック、シャットダウンフック、エラーフックの総称。
非信頼フック	SC3, SC4において、非信頼 OS アプリケーションに所属する OS アプリケーション固有のスタートアップフック、シャットダウンフック、エラーフックの総称。
システムサービス	OS が提供するサービスルーチン。
コンテナ	コンフィギュレーション時に記述するパラメータの集合。コンテナはコンテナ名称と 0 個以上の属性を持つ。また、コンテナは入れ子の形式でコンテナに含むことができる。これをサブコンテナと呼ぶ。 コンテナが OS オブジェクトのパラメータを記載する場合、特にオブジェクトコンテナと呼ぶ。
コンフィギュレーションクラス	指定したパラメータがどのタイミングで使用されるかを示す。種別は以下の 3 つである。 ・ プレコンパイルタイム プリプロセッサ実行時 ・ リンクタイム 各モジュールのコンパイルの終了後 ・ ポストビルドタイム ビルド終了後 コンテナで指定するパラメータ毎にコンフィギュレーションクラスが規定される。
プロセッサ	演算器やレジスタから構成されるハードウェアで、1 つ以上のプロセッサコアで構成される。
コア割付け	OS オブジェクトをマルチコアシステム中のどのコアで動作させるかを決定すること。
コア間排他制御	複数のコアに跨ったコンテキスト間での OS 内部データの一貫性を保つための排他制御。具体的にはアトミックな Test and Set 等によるロックを取得した上で内部データを操作するという規約を設けることで実現する。
コア内排他制御	単一のコア内のコンテキスト間での OS 内部データの一貫性を保つための排他制御。具体的には割込み禁止で実現する。

用語	定義
アトミック命令	変数の判断(テスト)と設定(セット)を不可分(アトミック)に行う「Test and Set」の概念を実現するメモリアクセス命令. 基本的な TAS(Test and Set)のほかに, CAS(Compare and Swap), LL/SC(Load Link/Store Conditional)といった各種の命令をさす.
スモールデータ領域	比較的小さなサイズの静的変数を配置するメモリ領域. スモールデータ領域に置いた変数は, グローバルポインタと呼ばれるレジスタからの相対アドレス指定によりアクセスすることで, アクセスを高速化することができる.
スモールデータ最適化	スモールデータ領域, グローバルポインタを使用した最適化.
割り込み処理コア	外部割り込みによって起動される ISR が動作するコア.
MPU	Memory Protection Unit(メモリ保護ユニット)の略語. 特定のメモリ領域アドレス, サイズ, アクセス方法を設定することで不正なメモリアクセスからメモリを保護するハードウェア.
組	メモリ保護ユニット(MPU)が監視可能な保護領域の数を計上するための単位. 仕様記述の便宜上, 定義するものである.
メモリセクション	メモリのソフトウェア面での役割(コード領域, データ領域, スタック領域など)で分類するメモリ領域の名称. メモリセクションはメモリリージョンに配置される. 一般的には, 単に「セクション」とも呼ばれる.
Overlay アドレス	マルチコア環境において, 各コアのアドレス空間中のある同じアドレス範囲に実体の異なるメモリを割付けたアドレス体系. 詳細は「次世代車載システム向け RTOS ハードウェア要求仕様書」参照.
アクセス権	OS アプリケーションに所属する処理単位が, メモリ, システムサービス, OS オブジェクトに対して操作可能かどうかを示す権限.
共有リード専有ライト領域	OS がメモリ保護機能を提供する場合に, OS メモリ保護の対象とするメモリセクションの1つ. すべての OS アプリケーションに読出しを許可するが, 特定の OS アプリケーションのみに書込みを許可する.
特権モードと非特権モード	プロセッサが持つ動作モード. 一般に, 特権モードではすべてのハードウェア資源にアクセスすることができ, プロセッサで定義されたすべての命令を実行できる. 逆に, 非特権モードでは一部のハードウェア資源しかアクセスできず, 実行できる命令が制限される.
GPT	General Purpose Timer の略語. 汎用的に使用できるタイマを指し, ドライバ仕様が AUTOSAR で規定されている.

用語	定義
ターゲット	次世代車載システム向け RTOS を実装する対象となるハードウェアと、実装に使用するソフトウェア開発環境の総称。
実行時間	- タスク タスクが実行状態となってから、休止状態か待ち状態になるまでの時間。タスク実行時間にはエラー処理、プレタスクフック、ポストタスクフック、システムサービスの実行時間を含む。タスクが実行可能状態になっている時間、カテゴリ 2 ISR に割込まれた場合の時間、プロテクションフックの実行時間は除く。カテゴリ 1 ISR に割込まれた場合の時間は、割込まれたタスクの実行時間に含む。 - カテゴリ 2 ISR カテゴリ 2 ISR が発生してから終了するまでの時間。カテゴリ 2 ISR 実行時間はエラー処理、システムサービスの実行時間を含む。より高い優先度のカテゴリ 2 ISR に割込まれた場合の時間、プロテクションフックの実行時間は除く。カテゴリ 1 ISR に割込まれた場合の時間は、割込まれたカテゴリ 2 ISR の実行時間に含む。
実行時間バジェット	タスクもしくはカテゴリ 2 ISR に許された実行時間の最大値。
OS 管理割込み禁止時間バジェット	タスクもしくはカテゴリ 2 ISR に許された OS 管理割込み禁止時間の最大値。
全割込み禁止時間バジェット	タスクもしくはカテゴリ 2 ISR に許された全割込み禁止時間の最大値。
リソース占有時間	タスクもしくはカテゴリ 2 ISR がリソースを占有する時間。ただし、より高い優先度のタスクやカテゴリ 2 ISR が実行されている時間は除く。
リソース占有時間バジェット	タスクもしくはカテゴリ 2 ISR に許されたリソース占有時間の最大値。
到着時間	- タスク タスクの起動もしくは待ち解除間隔。起動には休止状態から実行可能状態への遷移とタスク実行中の多重起動の双方を含む。 - カテゴリ 2 ISR カテゴリ 2 ISR の発生間隔。
タイムフレーム	タスクもしくはカテゴリ 2 ISR に許された到着時間の最小値。
経過時間監視	タイミング保護機能のうち、以下の監視機能をまとめた総称。 - 実行時間監視 - リソース占有時間監視 - 割込み禁止時間監視

用語	定義
到着時間監視	タイミング保護機能のうち、タスクの起動、待ち解除およびカテゴリ 2 ISR の発生間隔を監視する機能。
割込み要因	タイマのオーバーフローや電圧変化など、ハードウェア上で割込みを発生させる要因を示す。
割込み禁止状態	割込み禁止状態とは、 <code>DisableAllInterrupts</code> 、 <code>SuspendAllInterrupts</code> 、 <code>SuspendOSInterrupts</code> のいずれかを発行した状態を示す。逆にこれらを解除した状態を、割込み許可状態と呼ぶ。 <code>DisableInterruptSource</code> を発行した場合にも同様の仕様が適用される場合のみ特記事項として記載する。
全割込み禁止状態	<code>DisableAllInterrupts</code> 、 <code>SuspendAllInterrupts</code> のどちらかを発行した状態を示す。逆にこれらを解除した状態を、全割込み許可状態と呼ぶ。
OS 割込み禁止状態	<code>SuspendOSInterrupts</code> を発行した状態を示す。逆にこれを解除した状態を、OS 割込み許可状態と呼ぶ。
割込み禁止時間	タスクもしくはカテゴリ 2 ISR が、割込みを禁止してから許可するまでの時間。 - 全割込み禁止時間 すべての割込みに対する割込み禁止時間。 - OS 割込み禁止時間 すべてのカテゴリ 2 ISR に対する割込み禁止時間。
満了処理	アラームに接続されたカウンタが、アラームに登録されている満了点に達した際に実行される処理。同様に、スケジュールテーブルの満了点で実行される処理も指す。
動作中	システム、OS、コア、スケジュールテーブル、OS アプリケーションが動作している状態を指す。
実行中	タスク、ISR、フックルーチン、システムサービス、信頼関数、コンテキストが実行されている状態を指す。
操作中	<code>IncrementCounter</code> を実行中のカウンタの状態を指す。
セット済み	システムサービスによってアラームが満了するように設定された状態を指す。

変更履歴

Version	Date	Detail	Editor
1.0.0	2011/9/30	NCES 内部リリース	NCES
1.0.1	2011/12/28	ATK2 コンソーシアム向けリリース	NCES
1.0.2	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 ・ 用語を追加	NCES
2.0.0	2013/1/22	一般向けリリース	NCES