●はじめに

本仕様（案）は、μITRON 仕様 3.0 をベースとして、トヨタ自動車(株)第３電子技術部にて車載電子制御システム（ここではエンジン、トランスミッション制御を示す）用として必要と思われる機能についてまとめたものである。
リアルタイム OS 自動車応用技術委員会に対して、本仕様（案）を、

「μITRON3.0 仕様サブセット：自動車制御用リアルタイムＯＳ仕様（案）」

として提案する。

●標準化の意義

既に広く業界標準として使用されているμITRON3.0 仕様を、自動車制御応用分野に特化して標準化することは、CPU 選択自由度の向上、信頼性・品質の確保、デバッグ環境の整備、アプリケーションプログラムの標準化・ライフタイムの延長、等の面でメリットがあると考えられる。
これにより、自動車メーカとしては、低コストマイコンの早期投入や、アプリケーションプログラムの移植性向上による開発工数の低減効果等が期待できる。
また、応用分野毎にサブセット仕様が広く頒布され、流通することは、標準仕様から拡張された機能サポート時の適応化の面でも小回りがきくことになり、ユーザがメリットを享受できる機会が増えると考えられる。

●車載電子制御システム（以下ECU 制御システム）の要件

ECU 制御システムでは、ハードウェア・ソフトウェアの如何を問わず、一定のコスト制約があり、かつ徹底した信頼性が要求されることが多い。そのため、リアルタイム OS に許されるオーバヘッドは、CPU 性能・リソーセスの１％以下が望ましい。

●自動車用リアルタイムOS 仕様（案）の定義

本ドキュメント中では、μITRON3.0 仕様のうち、実装時に実際に ECU 制御システム開発に使用した、あるいは使用すると思われた機能群のことを「μITRON3.0 仕様サブセット：自動車制御用リアルタイム OS 仕様（案）」と呼ぶ。

●自動車制御用リアルタイムＯＳ仕様（案）の考え方

ECU 制御用としてのリアルタイムＯＳは、現状のμITRON3.0 仕様の範囲内で十分実現できると考えられる。ただし、前期の ECU 制御システムの要件を満たし、コスト制約と信頼性を両立させるには、ブラックボックスであるリアルタイム OS の機能範囲は極力小さくしておくことが望ましい。
具体的には、必要最小限のスケジューリング機能のみを実装することにより、必要最低限の割り込みハンドリング機能とマルチタスク実現のための機能を実現する。他の機能につ

いては、この最小機能構成をベースに、設計者が追加コンフィグレーションできる、あるいはライブラリとして作りだすことができるようになっていればよい。
従って、今回提案した自動車制御用リアルタイムＯＳ仕様（案）は、μITRON3.0 仕様のうち必要最小限の機能に限定し、コンパクトなメモリ消費量で、割り込みハンドリング及びマルチタスクを実現するための仕様（案）策定に重点をおくことを基本方針とした。特に、ＲＡＭについては実際のマイクロプロセッサでの搭載量を考慮し、機能の一部に制限を加えてでも、実装時の消費量を抑える方向で検討を行った。

●カーネル概要

ECU 制御システム用カーネルとしては、タスク状態は「実行 RUN」「実行可能 READY」「待ち WAIT」「休止 DORMANT」の４状態で十分であると思われる。
ただし､デバッグ時の利便性を考慮すると｢強制待ち SUSPEND｣｢二重待ち WAIT-SUSPEND」があると便利であるが、量産組み込み用のカーネルとしては必要ない。デバッグのための上記 2 状態を量産用カーネルに実装するかどうかは、コストや信頼性を勘案し、各応用システム毎に必要性を検討する必要があると思われる。
自動車制御用として選択したシステムコール一覧については後述する。μITRON の仕様範囲外となるが、簡易なメッセージ通信、イベント通知・同期制御機能も有用と思われたため、仕様（案）に追加することとした。

●コンテキスト退避領域の共有

プリエンプトによるタスク管理は、優先度に応じた割り込みハンドリングを実現するためには大変有効であるが、コンテキスト退避領域をタスク毎に持つ必要があり、ＲＡＭを大量に消費してしまうというデメリットも持つ。
ECU 制御システムの場合、プリエンプトの考え方は必要不可欠であるが、同一優先度内に複数タスクを割り当てる場合には各タスクがそれぞれ独立にコンテキスト退避領域を持つ必要はほとんどないと考えられる。そのため、仕様（案）では、同一優先度のタスクはコンテキスト退避領域を共有し、ＲＡＭ消費量を削減しつつ、割り込みレベルに応じたプリエンプトが実現できるコンテキスト退避領域の共有機能を検討することとした。
制限事項としては、優先度を動的に変更するシステムコールを発行できない、同一優先度内で実行可能状態にあるタスクの実行順序を変更できない、同一優先度に複数のタスクが存在する場合にそれらのタスクを待ち状態に遷移させる可能性のあるシステムコールを発行できない、等があるが、いずれも ECU 制御システム用としては問題ないと思われたため、仕様（案）に盛り込むこととした。

●システムコール一覧

機能分類		名称	機能
タスク管理		sta_tsk	タスク起動
		ista_tsk	タスク起動
		ext_tsk	自タスク終了
		ter_tsk	他タスク強制終了
		dis_dsp	ディスパッチ禁止
		ena_dsp	ディスパッチ許可
		rel_wai	他タスクの待ち状態強制解除
		irel_wai	他タスクの待ち状態強制解除
タスク付属同期		slp_tsk	自タスクを起床待ち状態へ移行
		wup_tsk	他タスクの起床
		iwup_tsk	他タスクの起床
		can_wup	タスクの起床要求を無効化
同期・通信	セマフォ	sig_sem	セマフォ資源返却
		isig_sem	セマフォ資源返却
		wai_sem	セマフォ資源獲得
		preq_sem	セマフォ資源獲得(ポーリング)
	イベントフラグ	set_flg	イベントフラグのセット
		iset_flg	イベントフラグのセット
		clr_flg	イベントフラグのクリア
		wai_flg	イベントフラグ待ち
		pol_flg	イベントフラグ待ち(ポーリング)
	キュー	vsnd_msq	キューへのメッセージ送信
		ivsnd_msq	キューへのメッセージ送信
		vrcv_msq	キューからメッセージ受信
		pvrcv_msq	キューからメッセージ受信(ポーリング)
		vsnd_dtq	キューへのデータ送信
		ivsnd_dtq	キューへのデータ送信
		vrcv_dtq	キューからデータ受信
		pvrcv_dtq	キューからデータ受信(ポーリング)
割り込み管理		ret_int	割り込みハンドラからの復帰
		ret_wup	割り込みハンドラからの復帰とタスク起床
		loc_cpu	割り込みとディスパッチの禁止
		unl_cpu	割り込みとディスパッチの許可
		dis_int	割り込みの禁止
		ena_int	割り込みの許可
		chg_icr	割り込み制御レジスタ変更
		ref_icr	割り込み制御レジスタ参照
時間管理	タスク遅延	dly_tsk	タスク遅延
	周期起動	act_cyc	周期起動ハンドラ活性制御
	ハンドラから復帰	ret_tmr	タイマハンドラから復帰

システムコール補足

キューへのメッセージ送信

【名称】vsnd_msq：Send Message to Queue　タスク

ivsnd_msq：Send Message to Queue for Interrupt Handoer　ハンドラ

【解説】キューＩＤで指定されたメッセージキューに対し、メッセージパケット先頭アドレスが示すメッセージパケットを送信する。キューで既にメッセージを待っているタスクがあった場合には、待ち状態から実行可能状態に遷移する。１つのメッセージキューに対し、メッセージ受信待ち状態にはいることのできるタスクは１つとする。メッセージキューはリングバッファによって実現する。

【パラメータ】キューＩＤ、メッセージパケットの先頭アドレス

キューからのメッセージ受信

【名称】vrcv_msq：Receive Message from Queue　タスク

pvrcv_msq：Poll and Receive Message from Queue（ポーリング）タスク／ハンドラ

【解説】キューＩＤで指定されたメッセージキューからメッセージを受信する。対象メッセージキューにメッセージが入っている場合、メッセージキューの先頭のメッセージを取り出す。１つのメッセージキューに対し、vrcv_msq によりメッセージ受信待ち状態にはいることのできるタスクは１つとする。（１：Ｎ通信は対象外）

vrcv_msq システムコールでは、対象メッセージキューにまだメッセージが到着していない場合、本システムコールを発行したタスクは待ち状態になり、対象メッセージキューへのメッセージ到着により実行可能状態に遷移する。

【パラメータ】キューＩＤ

【リターンパラメータ】メッセージパケットの先頭アドレス

キューへのデータ送信

【名称】vsnd_dtq：Send Data to Queue　タスク

ivsnd_dtq：Send Data to Queue for Interrupt Handler　ハンドラ

【解説】キューＩＤで指定されたデータキューに対しデータを送信する。対象データキューで既にデータを待っているタスクがあった場合、待ち状態から実行可能状態に遷移する。１つのデータに対し、メッセージ受信待ち状態にはいることのできるタスクは１つとする。データキューはリングバッファによって実現する。

【パラメータ】キューＩＤ、送信データ

割り込み制御レジスタ変更機能

【名称】vchg_icr：Change Interrupt Control register
【解説】割り込みハンドラ指定番号で指定された割り込み源に対応する割り込みコントロールレジスタの内容を割り込みコントローラコマンドの指定に従って変更する。
【パラメータ】割り込みハンドラ指定番号、割り込みコントローラコマンド
割り込みコントローラコマンドの種類

- ・割り込み制御レジスタの割り込み要求フラグをクリアする
- ・割り込み制御レジスタの割り込みマスクを解除する
- ・割り込み制御レジスタの割り込みをマスクする
- ・割り込み制御レジスタの割り込みレベルを'数値'で指定した値に変更する

割り込み制御レジスタ参照
【名称】ref_icr：Refre Interrupt Control register
【解説】　割り込みハンドラ指定番号で指定された割り込み源に対応する割り込みコントロールレジスタの内容を、割り込み制御レジスタの内容で指定された領域に格納する。
【パラメータ】割り込みハンドラ指定番号
【リターンパラメータ】割り込み制御レジスタの内容
以下のパラメータとの論理積を取ることによって評価。

- ・割り込み要求フラグ
- ・割り込みマスクフラグ
- ・割り込みレベル