これから10年使える技術！
標準AUTOSAR開発プラットホーム入門

安全に使い回す！車載ソフトウェアの世界

第12回　クルマ用OSの安全メカニズム②…タイミング保護

高田 光隆

● 今回紹介すること

クルマ用標準OS「AUTOSAR OS」には，安全に使うために，アクセス保護（メモリ保護）とタイミング保護（時間保護）の仕組みが用意されています．前回はアクセス保護の仕組みを紹介しました．

今回は，もう1つの保護機能であるタイミング保護の仕組みを紹介します．AUTOSARには，保護機能の有無で幾つかのクラス（スケーラビリティ・クラスSCx）が用意されていますが，そのうちSC2とSC4に搭載されています．

安全に使うためのもう1つの機能「タイミング保護」

● OSの機能として用意されている理由

車載ソフトウェアでは，アプリケーションの時間要求があります．決められた時間内に処理を必ず終えるために，リアルタイム性を確保（保証）する必要があります．

一般に，組み込みシステムでは，ある処理区間の最悪実行時間を見積もることができるリアルタイムOSを使用します．

ところがAUTOSARのようにソフトウェアの再利用も目的としているソフトウェア・プラットフォームを使うときは，話は少しややこしくなります．全て自前でソフトウェアを開発できればよいのですが，外部からの購入品や再利用したソフトウェアの中には設計の意図通りに振る舞わない（決められた時間内にタスクを終えない）ソフトウェア・モジュール（SW-CやCDD）を使ってしまうことがあります．

OSのアラーム機能や，ソフトウェア・モジュールのウォッチドッグ機能（スケジュール・テーブルやBSWにある）を使えば，ある決められた処理の時間計測（チェック）を行うことはできますが，全てのタスクにおいて時間のチェックを行うのは大変ですし，計測する処理区間ごとにOSのリソースを消費してしまいます（**図1**）．

そこで，OSに時間保護機能を追加し，ソフトウェアの設計時に時間要求を設定できるようにしてあります．時間要求を満たさない処理が出て来たときにOSが検知して，時間保護違反処理を行ってくれます．

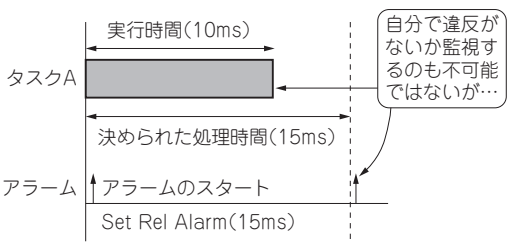

図1　ユーザ・プログラムでタスクの処理時間をチェックして監視することも不可能ではないが，すべてのタスクをチェックするのは大変

● 動作イメージ

▶タスクの処理時間が設計通りの場合

例えば**表1**のようなタスクの設定があったとします．

時間0のときに全てのタスクが実行可能状態になっているとすると，タスク実行は**図2**のようになります．

この場合は全てのタスクは当初の設計通りに動作が行われています．

▶タスクの処理時間が設計通りではない場合

さて次に，例えばタスク実行中の割り込み処理に思った以上に時間がかかってしまったなど，何らかの影響でタスクAとタスクBの時間が増えたとします．

(1) タスクBの実行時間が増えたせいで，
(2) 本来ならばタスクCが動く時間でタスクA，Bが実行されました．
(3) Cの実行時間が遅れたため，タスクBの次の周期までタスクCの処理が終わっていません．
(4) タスクCが残りの処理を行っても周期（15）で終わりきらずにまたタスクCが呼び出されることになってしまいます．

表1　想定してみるタスクの設定

タスク名	優先度	実行時間	起動周期
A	高	1	5
B	中	3	10
C	低	5	15

第3回　実験のハードウェア＆使用した車載マイコン（2016年3月号）
第4回　実験のソフトウェア（2016年4月号）
第5回　ソフトウェアの全体的な構成／仕様を決める…全体システム設計（2016年5月号）