

OSEK/VDX仕様からAUTOSAR OS仕様への拡張

2008/11/20

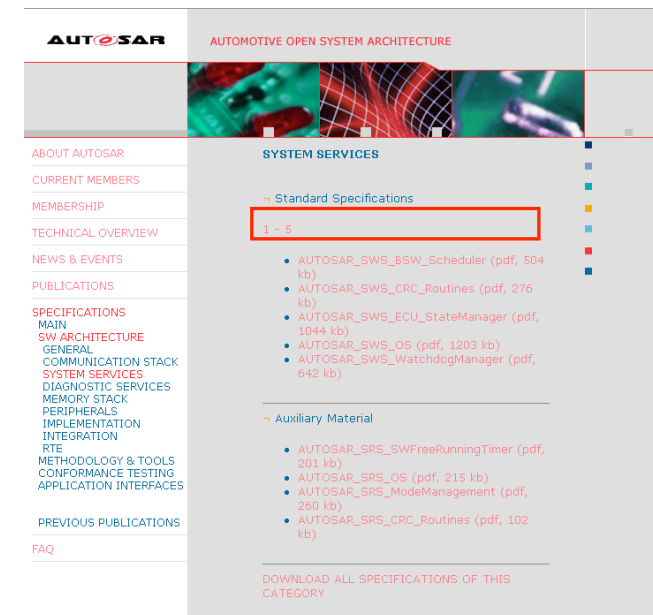
株式会社ヴィッツ 組込みソフトウェア開発部

杉本明加

アジェンダ

- TOPPERS Automotive KernelをAUTOSAR OS仕様 SC2へ拡張する方法について解説します。
 - AUTOSAR OS Version2.0.1仕様はAUTOSAR※から仕様が公開されているリアルタイムOS仕様です。
 - TOPPERS Automotive Kernelはヴィッツが開発し、2004年よりTOPPERSプロジェクトから公開されている (旧称) TOPPERS/OSEKカーネルの最新リリースです。

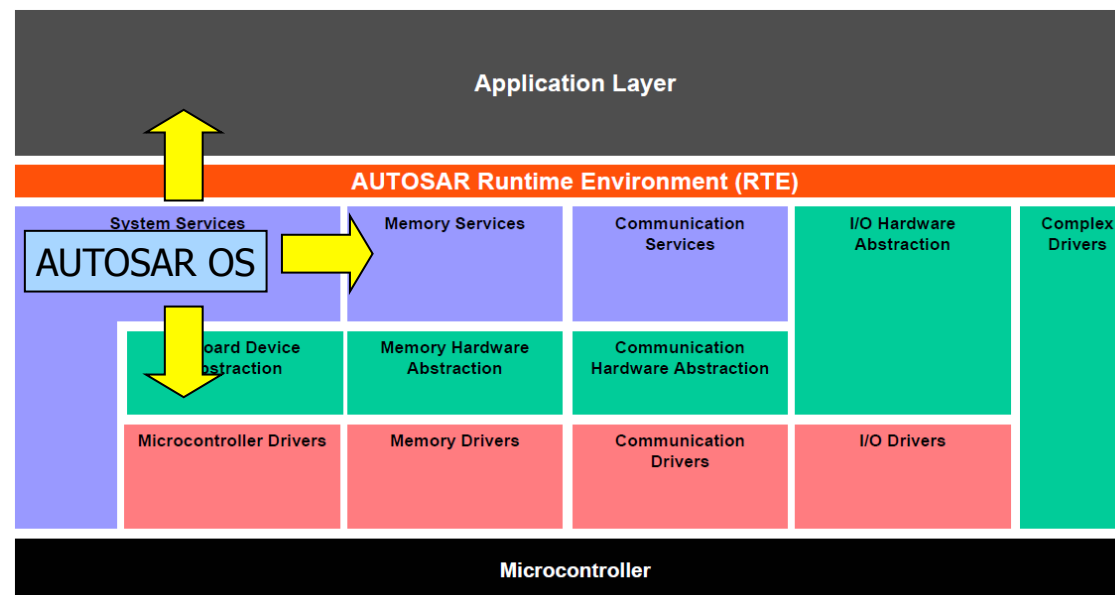
- 解説内容
 - AUTOSAR OS仕様の紹介
 - 機能構成の紹介
 - 各機能の機能概要/実装方法の紹介
 - まとめ



※ <http://www.autosar.org>

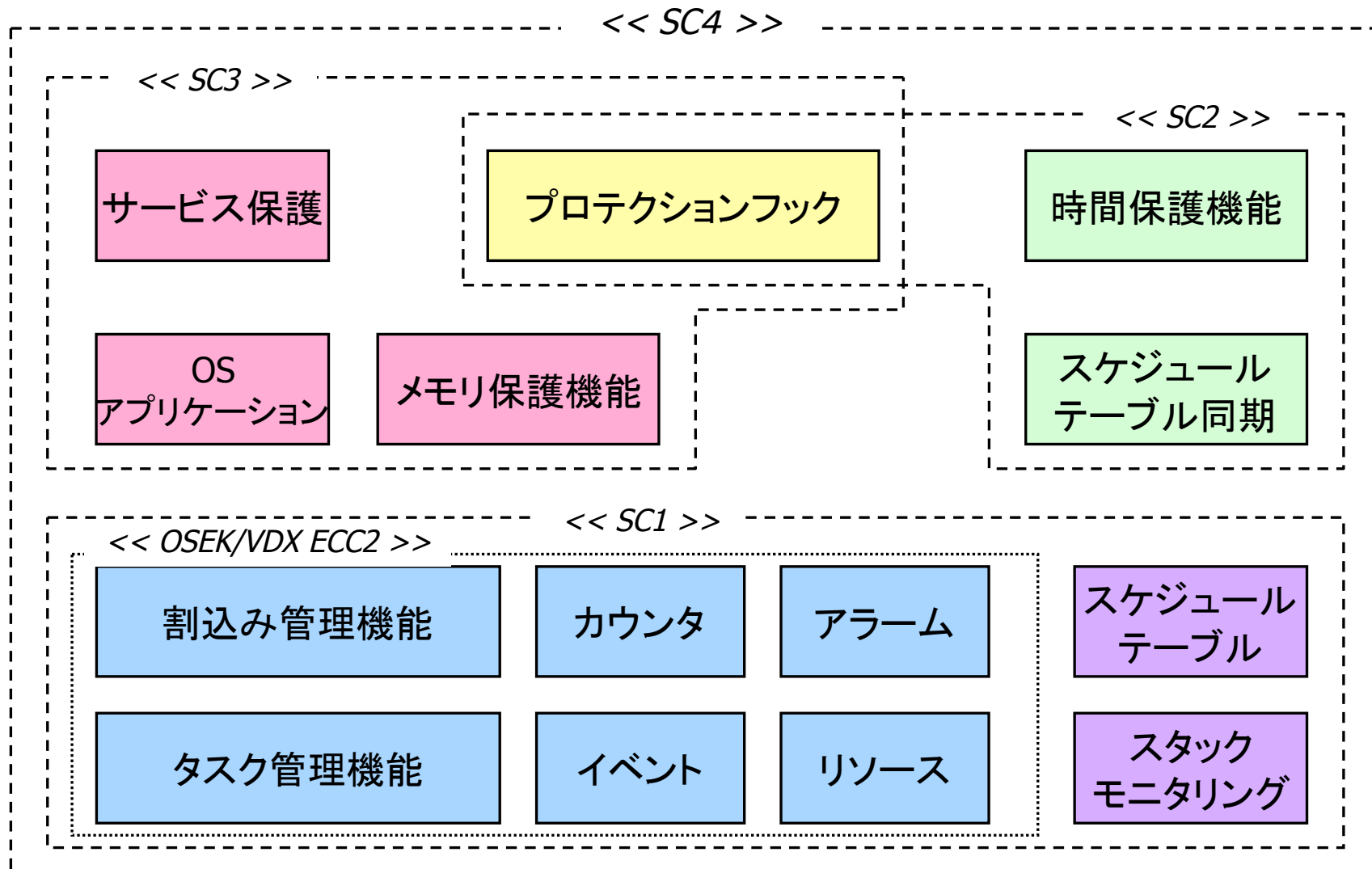
AUTOSAR OS仕様

- AUTOSARフレームワークのコンポーネントの1つ
 - AUTOSAR自体はアプリケーションモデルからデバイスドライバまで幅広く規定
 - OSはアプリケーション層やBSW(Basic SoftWare)にサービスを提供
- OSEK/VDX Ver2.2.3、ECC2をベースに機能拡張
 - 下位互換性は保証



Layered Software Architectureより抜粋

AUTOSAR OSの機能構成

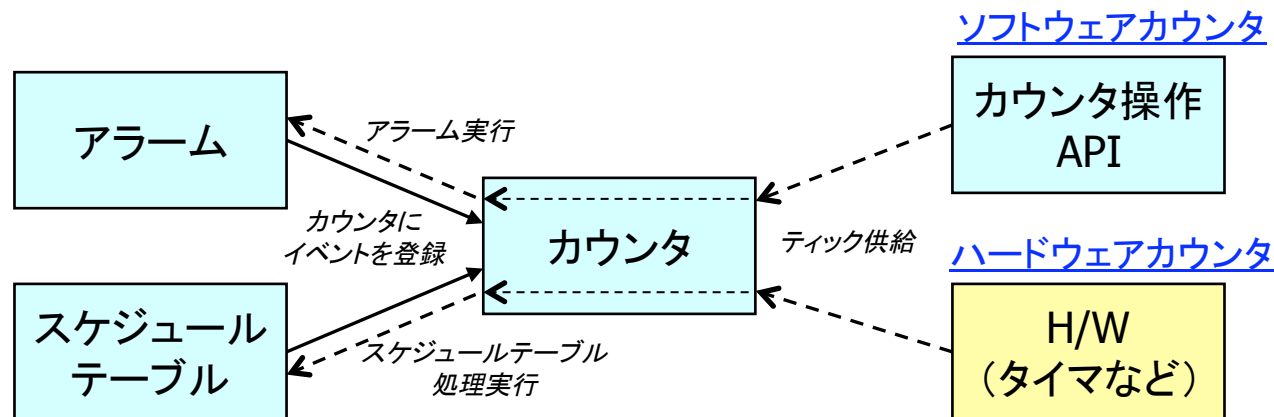


※ SC・・・Scalability Class

ヴィッツではSC2までを実装・評価

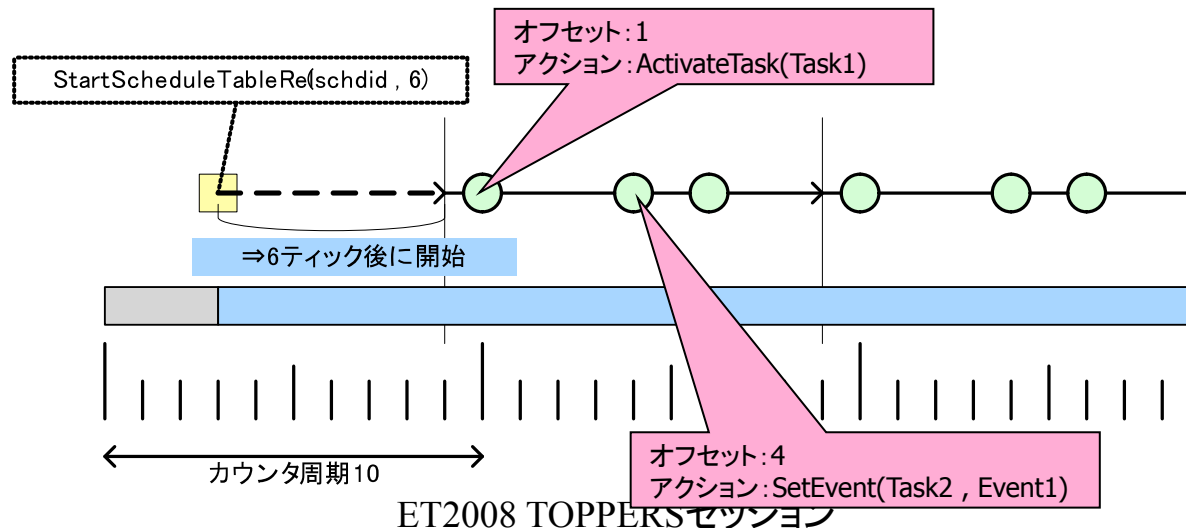
カウンタ機能の改良

- カウンタ操作APIの標準化
 - IncrementCounterがOS仕様で規定されたため、TOPPERS Automotive Kernel拡張のSignalCounterを廃止
- アラーム機能からの分離
 - カウンタ機能がアラーム機能と結合されていたため、スケジュールテーブルから使用できるように分離
- ハードウェアカウンタI/Fの定義
 - 従来のAPIによるカウンタ駆動に加えて、ハードウェア（e.g. タイマ）によってカウントするI/Fを追加



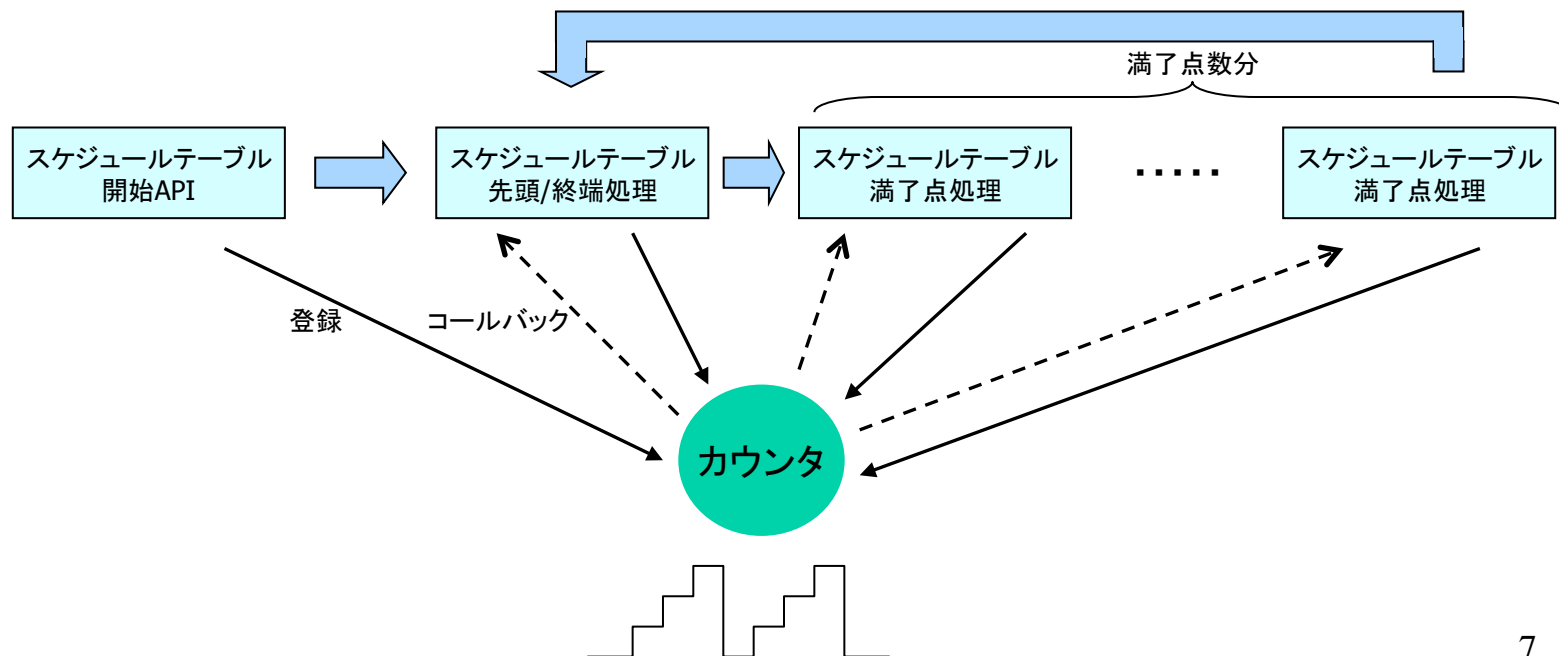
スケジュールテーブル＋同期機能

- 静的に定義されたアラームの集合
 - スケジュールテーブルは周期を持つ
 - スケジュールテーブルは先頭時刻からのオフセットと動作を定義した満了点を持つ
 - タスク起動
 - イベントセット
 - × コールバックルーチンは使用不可
- スケジュールテーブル同期
 - 外部の時刻ソースとスケジュールテーブルの時刻を同期する
 - 例えば、MCUのタイマとFlexRayのネットワーク時間の同期
 - 同期がずれた場合、満了点の間隔を増減して時刻を調整



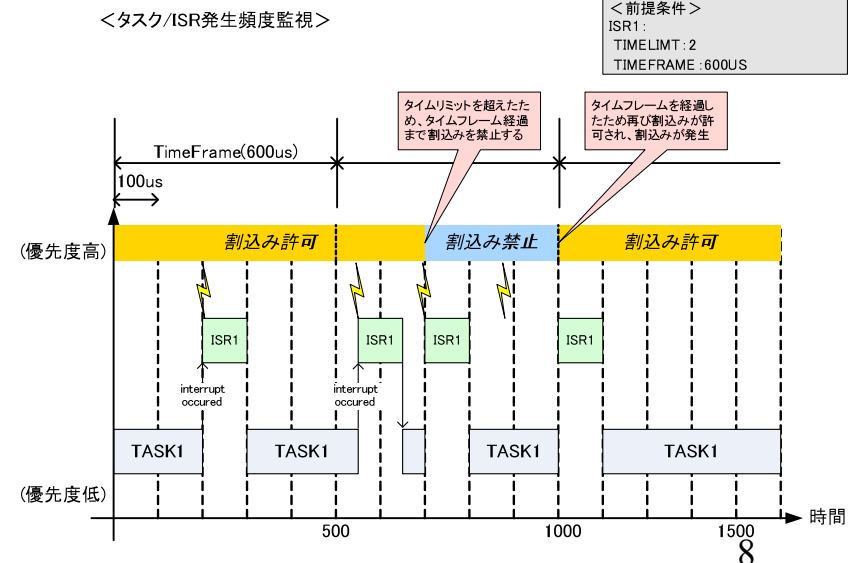
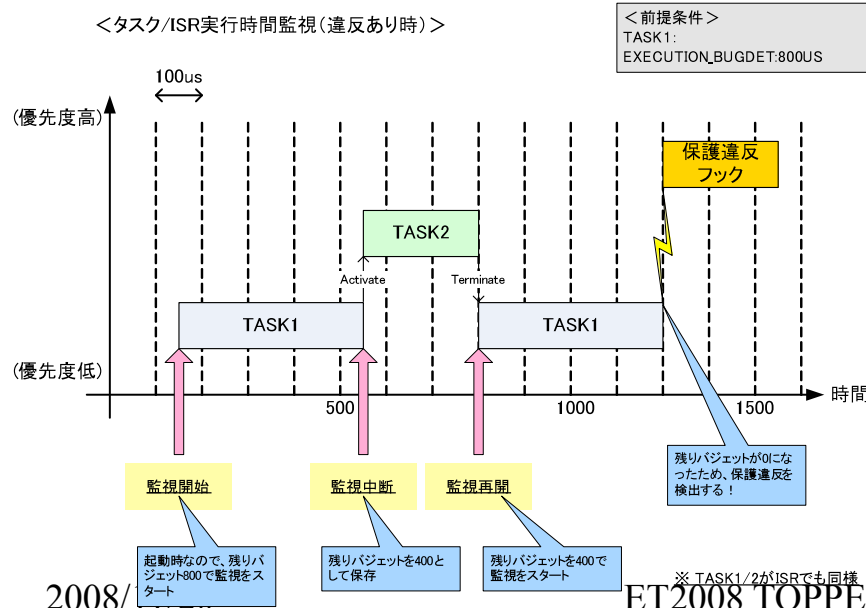
スケジュールテーブル＋同期機能

- カウンタからのコールバックの集合として実装
 - 各ポイントでの処理を実行した後、再度カウンタに次回コールバックを登録
 - 先頭/終端処理・・・スケジュールテーブル状態設定
 - 満了点処理・・・アクションの実行、同期補正処理実行



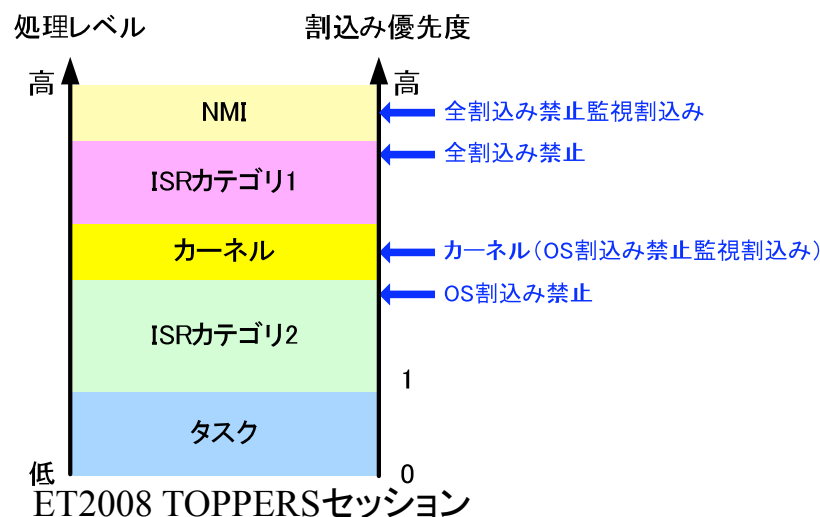
時間保護機能

- タスク/ISRカテゴリ2の動作を監視し、違反があった場合にプロテクションフックを呼び出す
 - タスク
 - 連続実行時間の監視
 - 特定時間内における実行積算時間の監視
 - リソース取得時間の監視
 - 割込み禁止時間の監視
 - ISRカテゴリ2
 - 連続実行時間の監視
 - 特定時間内における割込み発生頻度の監視
 - リソース取得時間の監視
 - 割込み禁止時間の監視



時間保護機能

- 保護監視タイマの導入
 - タスク/ISRカテゴリ2が実行時間違反/OS割込み禁止時間違反/リソース取得時間違反を起こしたときに割込みを発生する
 - タスク/ISRカテゴリ2が全割込み禁止時間違反を起こしたときに割込みを発生する
- タイムイベントヒープの導入
 - 並行して複数の保護違反イベントを監視するため、イベントの順序管理が必要となる
 - タスクディスパッチ、ISRカテゴリ2発生/復帰時にヒープにイベントを登録
 - 先頭イベントの場合は保護タイマを操作
- カーネルで使用する割込み優先度レベル
 - ISRを監視するために、割込み優先度をカーネルが予約する必要がある

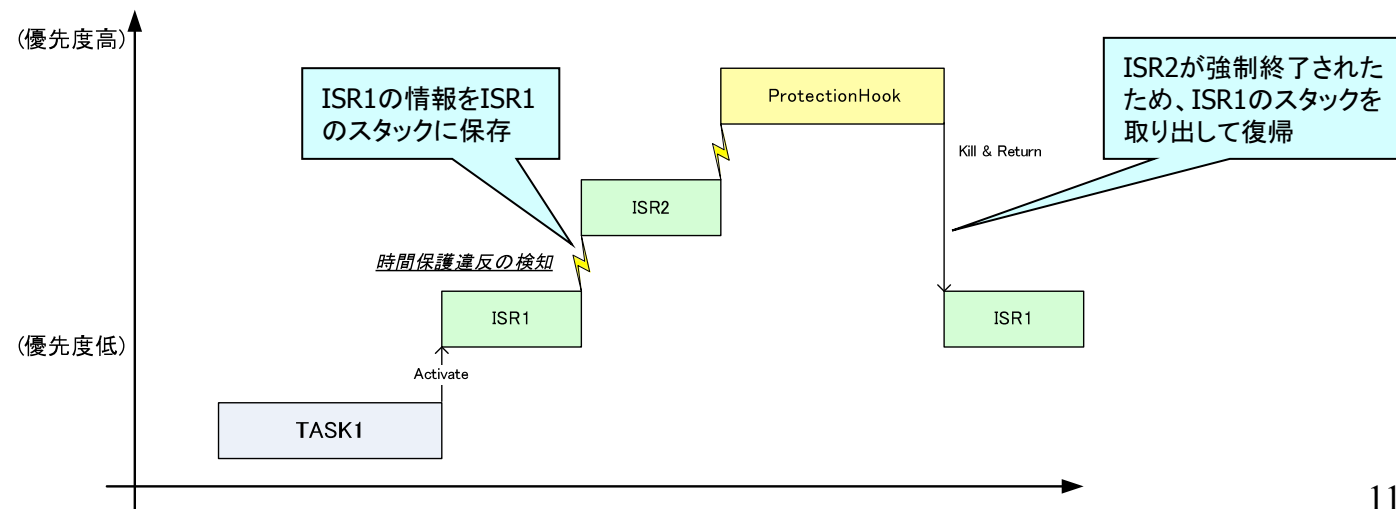


プロテクションフック

- 保護違反が発生した場合、ユーザの定義したルーチンを呼び出してエラーハンドリングを提供
 - 時間保護違反
 - メモリ保護違反
 - ⇒ SC3、SC4機能のため、説明省略
- プロテクションフックの返り値をチェックし、違反元オブジェクトに対していずれかの処理を実行
 - タスク/ISRカテゴリ2の強制終了
 - タスクの操作したオブジェクト状態も初期化
 - OSシャットダウン
 - OSアプリケーションの終了
 - ⇒ SC3、SC4機能のため、説明省略
 - OSアプリケーションの終了+タスク再スタート
 - ⇒ SC3、SC4機能のため、説明省略

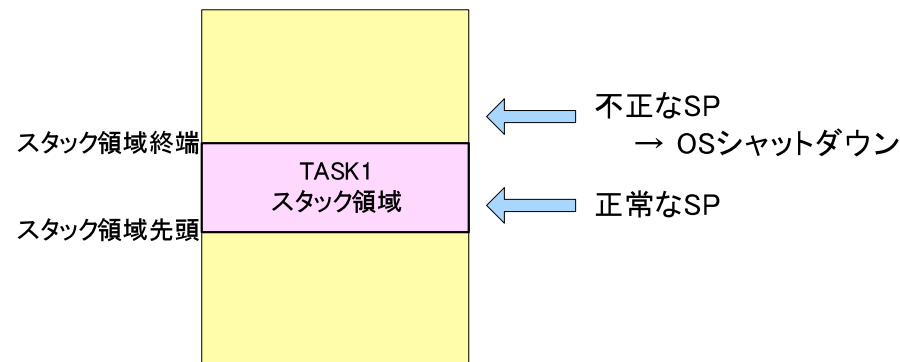
プロテクションフック

- タスク/ISRカテゴリ2の強制終了の実装
 - タスクをレディキューから外しやすくするため、データ構造を単方向リストから双方向リストへ変更
 - リソース解放機能の実装
 - タスク/ISRカテゴリ2が操作したリソースの管理情報を元に戻す
 - 割込み禁止状態のリセット機能の実装
 - 割込み発生時情報の保存/復帰の実装
 - ISRカテゴリ2が強制終了された場合、前段のISRのスタックに格納された情報(割込み元のレジスタ情報など)から割込んだコンテキストを復帰する必要がある



その他

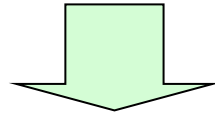
- スタックモニタリング
 - 以下のタイミングでスタックポインタをチェックし、オーバーフローしていればOSシャットダウン
 - タスクディスパッチ時
 - ISR2実行開始時
 - ただし、一度スタックオーバーフローした後に正常範囲にスタックポインタが戻った場合は検知不可能



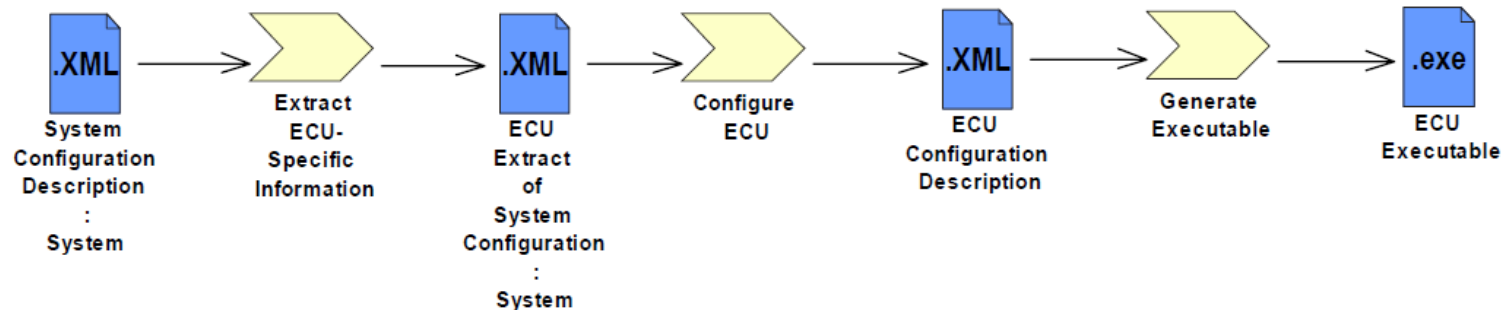
- 割込み管理機能拡張
 - 個別割込みの禁止/許可

コンフィギュレーション方法の変更 株式会社 ヴィッツ

- OSEK/VDX仕様でのコンフィギュレーション
 - OILによるテキストベース記述



- AUTOSAR OS仕様でのコンフィギュレーション
 - コンフィギュレーションツールによる設定
 - XML形式で出力
 - XMLを解釈してコンフィギュレーションファイルを生成
 - 従来のOILからXMLに変換する機構も実装



[AUTOSAR Technical Overviewより抜粋](#)

- TOPPERS Automotive Kernelをベースに機能修正、追加を行うことでAUTOSAR OS仕様への対応が可能です
- 既にいくつかのターゲットへのポーティング、評価実施済み
 - 仕様適合検証
 - 性能評価
- 最新仕様であるAUTOSAR OS Version 3.0.1へも対応中です

MEMO
