SCIOPTA

セイフティー・クリティカル・アプリケーション
のためのシステムソフトウエア

製品情報

IEC61508 セイフティー・クリティカル　リアルタイムカーネル

機 能 概 要

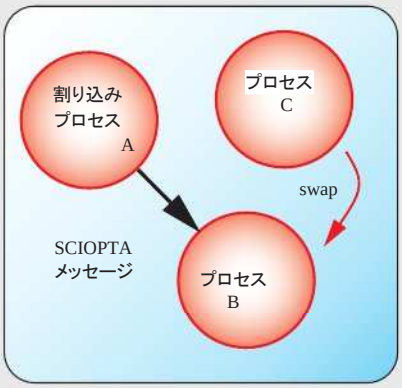
- メッセージベース・アーキテクチャ
- ハイパフォーマンスと低いメモリー フットプリント
- SCIOPTAシステムのすべてのデーター カプセル化され、メッセージ交換
- 非シェアードメモリーとグローバルデーター
- SCIOPTAメッセージはIDを所有
- SCIOPTAメッセージ自体は、所有権を持つ
- メッセージ所有者のみがアクセス可能。 従って、メッセージデータは、常に、 同時アクセスから保護
- メッセージ受信を選択可能
- SCIOPTAメッセージによる効率的な メモリー管理により、メモリーの断片化が 回避
- 複数の開発者でも、容易なシステム設計で きちんとしたメッセージインターフェース 確保
- システムデバッガは、メッセージのトレース システム検証、メッセージ・プールの分析 が可能
- エラーハンドリング処理

特 定 な 安 全 機 能

- すべてのカーネルデータ(コントールブロック とリスト)が反転され、2倍の格納をし、 1つのコピーは反転
- 安全なタイプ(例えば、セーフ・インテジャー) ダブル反転格納
- プログラムフローコントローラ
- メッセージパッシング上の妥当性をチェック する安全なプロセス間通信をご提供
- 安全なメモリー管理システムは、 同じCPU上に存在する非安全なシステム と安全な関連システムを区分が可能

テクノロジー

SCIOPTA IEC61508は、プリエンティブなマルチタスク、かつ、ハイパフォーマンスなリアルタイムカーネルが含まれています。多くの組み込み安全セイフティ機能を提供します。そして、SCIOPTAは非常によく使用されるセイフティ・クルティカルなアプリケーションに適しています。



ダイレクト・メッセージパッシンジを使用することによって、明確かつ簡単な設計から安全なシステムをつくり出すことができます。

割り込みプロセスAは、メッセージを割り当て、プロセスBに送信します。
それを待っているプロセスBは、実際は走っているプロセスCよりも優先順位が高い場合、カーネルはプロセスBにメッセージのリセーブを解放をします。

IEC 61508 認 証

SCIOPTAは以下の機関で認証されています。

TÜV Süd Munich

IEC 61508 SIL3(Safety Integrity Level 3) 構築

SCIOPTA セーフティ・ドキュメンテーションは、TÜV 認証報告書とセーフティマニュアルを含んだTÜV認証 を保障します。

非シェアード・メモリー実現

シェアード(共有)メモリー利用は、従来のリアルタイムOSにおけるプロセス間通信のための方法として利用してます。

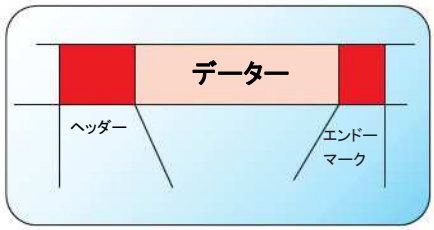
ユーザーは、セマフォといっしょに、シェアードメモリーを関連づけさ、完全なりスポンスを持ち、そして、セマフォは、データー領域とタイプをフルに関連させてきました。

SCIOPTAダイレクトメッセージパッシングではシェアードメモリーは必要ありません。
すべてのデーターは、メッセージをカプセル化され、カーネルがこれらのデーターを保護します。

安全なデーター・トランスファ

SCIOPTAメッセージは、プロセス間通信と仕組みに排他的に制御されています。

ダイレクトメッセージパッシングといっしょにプロセス間のデーター・トランスファを安全かつ簡単に行い多くのエラーチェックの構築も可能です。



SCIOPTAメッセージのヘッダーの構成は、SenderのプロセスID、所有者とアドレス、カーネルによってチェックされたデータ領域の任意サイズとエンドマークとなります。

簡単なコマンド

SCIOPTAメッセージパッシングのプロセス間通信は4つのシステムコールによって行うことができます。

- sc_msgAlloc
- sc_msgFree
- sc_msgTx
- sc_msgRx

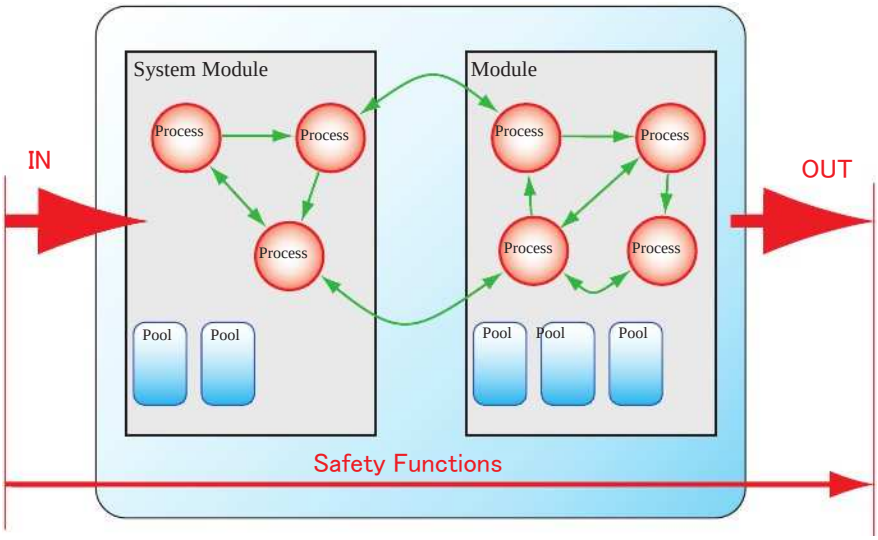
安 全 関 連 シ ス テ ム

SCIOPTA IEC61508 カーネルは、
IEC61508標準のPart1からPart7規格に
準拠しています。

重複データーストレージなどの特定安全機能、
プログラムフロー制御、スタック・チェック、
Crcファンクション、セイフデータータイプと
CPUチェックは90%以上の安全側故障割合が
結果として求められます。

これらの機能は、特別に構築されたデータを
過剰にメモリーチェックをせず、SIL2のために
シングルチャネル（CPU）を構築することを
許可が可能です。

SCIOPTA の開発手法やライフサイクル活動
は、IEC61508 のSIL3に基づいた認証されてます。
また、マルチチェネル（マルチCPU）システムでの
SCIOPTA61508を利用できることも
認証されています。

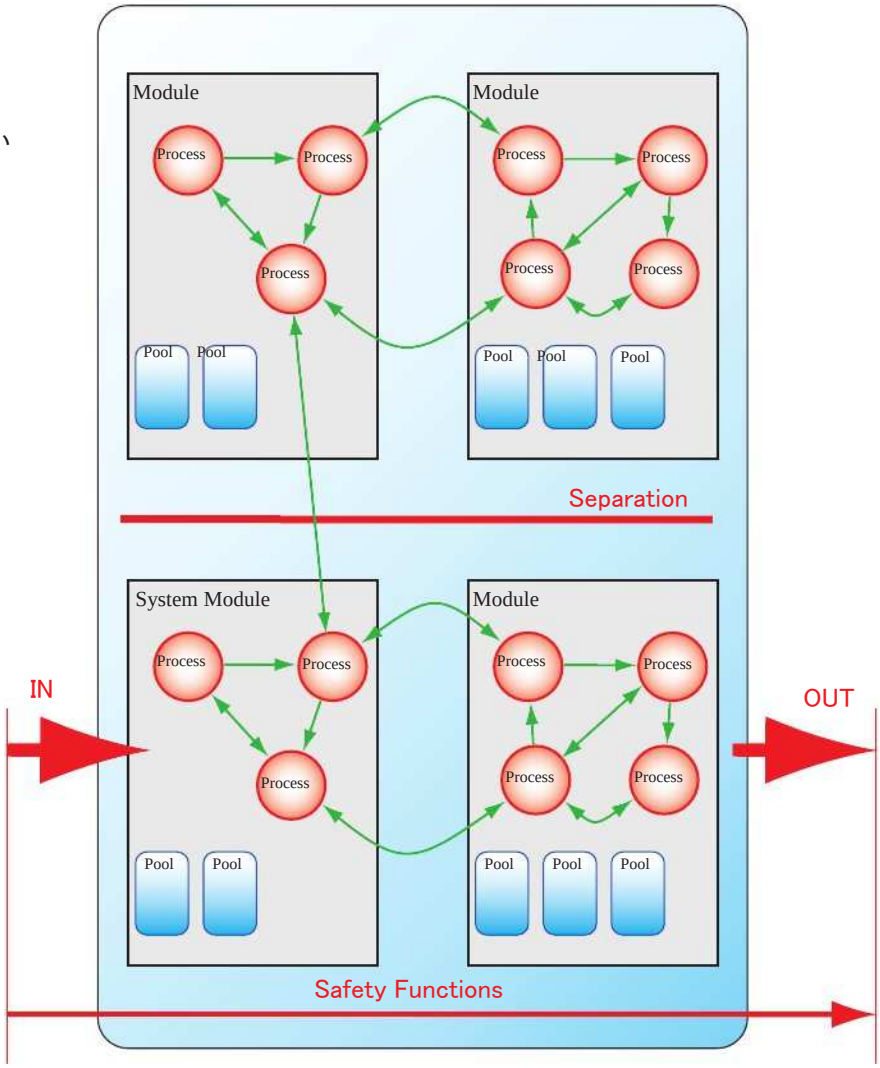


実 装 安 全 性 と 非 安 全 機 能

IEC61508-2 (7.4.2.3) で記載:

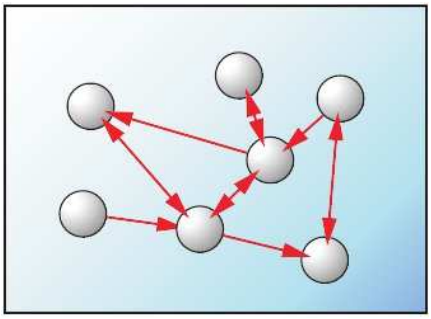
"電気/電子/ PEの安全関連システムは、
安全性機能と非安全性機能の両方を実装します。
それが安全と非安全性機能の実施が、ハードウエア
及びソフトウエアにおいて、十分に安全とされていない
部分は、独立した実装をすべきです。
（すなわち少しの安全な機能の不足も
安全の機能の危険な不足を引き起こさないために、
切り離されなければなりません）」"

重複データストレージ、プログラムフロー制御、
スタックチェック，crcファンクション，
安全データ・タイプとCPUチェックなど、
特定の安全機能を管理システムの条件を
満たすために、SCIOPTAのメモリー管理機能
を利用することにより、
それらの要求に答えることが可能です。



安全なプロセスフロー

安全カーネルは、プロセスフローの正当性を保証するために不正な処理の流れを検出し、内部および外部の安全機能を提供しています。つまたは複数の並列フローの論理プログラムの流れの監視がサポートされています。



実 行 制 御

SCIOPTAシステムでは、ユーザーが独自の関数を特定のシステムイベントでフックを呼び出し、それらを含めることができます。たとえば、メッセージはフックを送信します。メッセージはフックとプロセス交換フックを受け、証明されたシステムの重要な安全機能である場合、実行制御を認識するユーザーを許します。

集中したエラー処理

一元化されたエラー処理は、SCIOPTAの重要な安全機能です。すべてのエラーは、**Error Hook**と呼ばれる一元化されたエラー関数を呼び出します。

SCIOPTA カーネルは、エラーコードを単純にユーザーへ返すのではなく、ユーザーへエラーハンドリングの責任を持たせます。

セイフティ・メモリー・マネジメント

プロセスは、SCIOPTAモジュールとしてまとめることが可能です。各モジュールは最大128プールまで 、SCIOPTAのメッセージを保有可能です。

SCIOPTA は、モジュール・フレンドリーシップという概念があります。ユーザーは、モジュール間の定義や構築を設定できます。例えば、モジュールが境界線を横切ってきたとき、メッセージがコピーされるか定義できます。例えば、モジュールとプールのメモリーセグメントを同じロケーション、もしくは、異なるロケーションに配置するか定義できます。

SCIOPTA メモリー管理システム (SMMS) とハードウエアが所有メモリー管理Yニット(MMU) によって、完全なるメモリー保護を成し遂げることができます。

重要なデータ保護

セイフティ・カーネルは、内外のデータの保護を確実にするための機能を提供します。セイフティー・クリティカルなデーターは毎回読み込みと書き込みを行い、重要なデータは検証されます。すべてのカーネルデーターは格納されます。

カーネルは、安全なデータータイプのシステムコールを発行し、スタックデータは、プロセスが実行されていない間、保護されます。

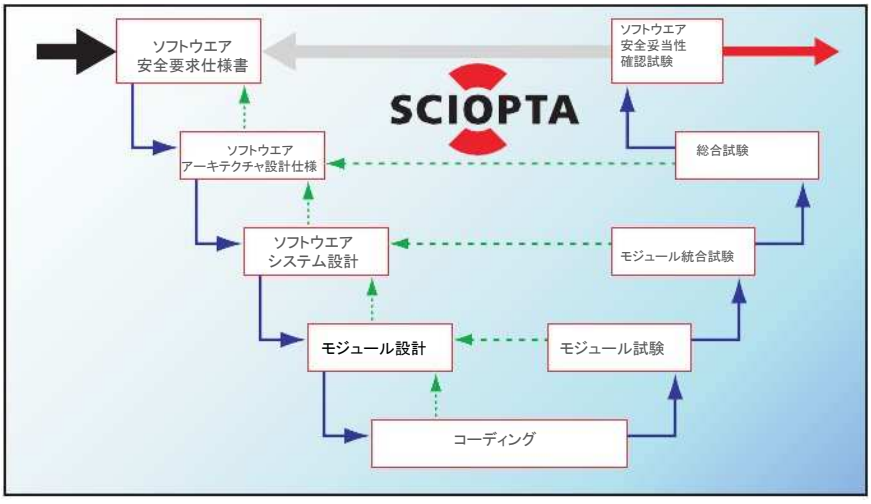
メッセージ・プロテクション

セーフティ・カーネルは、メッセージデータのデーターを完璧に情報チェック及び更新ができ、SCIOPTAのメッセージ保護を提供。メッセージ内部データは、カーネルによってチェックされます。すべてのチェックは、メッセージパッシングで実行されます。

コード・プロテクション

セイフティー・カーネルは、コードの保護するために、CRCファンクションを供給します。カーネルのコード保護は、プロジェクトの全体的なコード保護の一部です。

セイフティ ・ライフサイクル

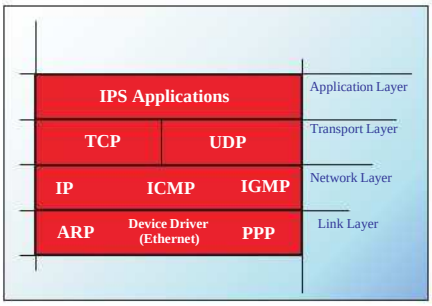


IECは61508の要件と活動、それに基づいて特定の安全ライフサイクルアプローチに基づいています。SCIOPTAライフサイクル活動とメソッドは、TÜVに認定されているIEC 61508規格SIL3に準拠します。

セイフティ・マニュアル

SCIOPTA IEC61508はは安全マニュアルを含みます。

SCIOPTA IPS (TCP/IP)



SCIOPTA IPSが具体的に組み込みシステムのインターネットプロトコルネットワークアプリケーションの要件を満たすように設計されています。これが持つ伝統的なインターネットスタック上でのIPSの優位性を与える高い性能と低メモリフットプリントを実現。

SCIOPTA IPS アプリケーション

SCIOPTA IPSは、 Web-Server, SMTP, FTP,TFTP, DNS, DHCP, Telnetなどの標準ネットワークアプリケーションをサポート。

SCIOPTAフラッシュ・ファイルシステム

予想外のリセットクリーンをハンドリングするためにテストされ、デザインされた高機能ファイルシステムです。
すべてのNOR, NAND,シリアルフラッシュタイプの利用が可能です。

SFFSは、NORを利用する組み込みや高度な信頼性を必要とするNANDフラッシュデバイスに利用されます。
システムの予想外の停電またはリセットから完全データ保護をします。

USB ホスト

SCIOPTA USBホスト・スタックは、コアコントロールデバイスドライバー、低レベルコミュニケーションAPIから高レベルクラスドライバまで含みます。

USB 1.1と2.0ホストコントロールとして、UHCI, OHCI , EHCIタイプをサポート。
これらのコントローラ・タイプは、ベンダー,やモデルに関係なく、常にサポート。

USB デバイス

SCIOPTA USB デバイスを利用してUSBデバイス経由で、SCIOPTAターゲットシステムと接続が可能です。

デバイスクラスは、フラッシュドライブにポータブルハードドライブ、
メモリカードリーダー、ジタルカメラ
ジタルカメラ、デジタルオーディオプレーヤー
使用されるUSB大容量ストレージデバイスクラスを含みます。

FATファイルシステム

組み込み用FAT12, FAT16 , FAT32対応ファイルシステムをサポート。
長いファイル名、キャッシングオプション, Unicode サポート、Compact Flash, MMC, SDカードのためのドライバー、HDD、NANDフラッシュやシリアルの組み込みフラッシュをターゲットにしたファイルシステムなどに利用可能です。

CPUのサポート

-ARM7/9/11

-ARM Cortex A3

-ARM Cortex R4

- Freescale ColdFire

- Freescale PowerPC MPC500
- Freescale PowerPC MPC55xx
- Freescale PowerPC MPC5200
- Freescale PowerPC MPC8xx
- Freescale PowerPC MPC82xx
- Freescale PowerPC MPC83xx

- AMCC PowerPC MPC400

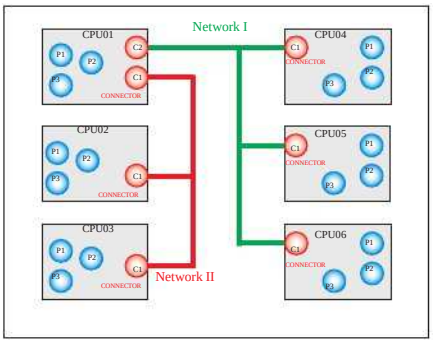
-Marvell Xscale

-ルネサス RX6xx

-ルネサス M16/32C

他のCPUについては問い合わせ下さい

透過分散システム



CONNECTOR は、異なるCPU環境にて透過分散を、SCIOPTAコミュニケーションプロセスで実現させます。

CONNECTORは、SCIOPTAカーネルが各CPUにサポートされ、マルチCPUシステムが実現できます。
互いのノードは、CONNECTOR プロセスによって制御されます。この制御は、ネットワーク通信システムのプロセスタスクの分散制御の知識に似ています。
SCIOPTAのインターフェースの土台は、クリーンなメッセージであり、あたかもシングルCPUシステムのように簡単に迅速にデザインができる分散システムの構築が可能です。

問い合わせ先

ポジティブワン株式会社

〒150-0043東京都渋谷区道玄坂1-12-1
渋谷マークシティ・ウエスト22F
Tel. 03-3256-3933
Fax 03-4360-5301

poc_sales@positive-one.com
www.positive-one.com