highintegritysystems

WITTENSTEIN

SAFERTOS® 拡張セキュリティモジュール (ESM)

SAFERTOS® 拡張セキュリティモジュール（ESM）は、安全かつ信頼性の高い実行環境を実現し、組込みアプリケーションを保護することを目的として開発されました。ESM は各ユーザーモードタスクの周囲に保護レイヤーを形成し、脅威が拡散する前に検知・隔離します。万一タスクが侵害された場合でも、攻撃の影響を最小限に抑え、システム全体を保護します。

車載システム向けのセキュリティを想定して設計された ESM は、自動車サイバーセキュリティに関する国際規格である ISO 21434 に準拠しています。

ESM の利点

- 脅威の検出
- 脅威の封じ込め
- データの保護

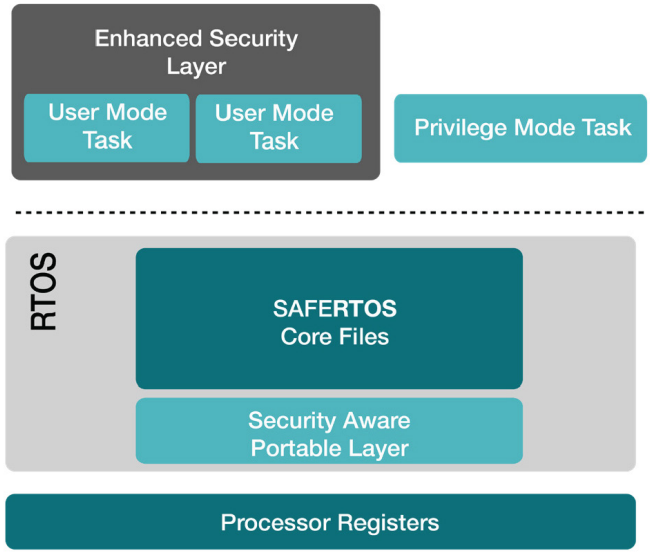

図 1. 拡張セキュリティモジュール
SAFERTOS とセキュリティ対応ポータブルレイヤー

ESM の特長は、その効果的な封じ込め戦略にあります。
主な目的は、侵害されたユーザーモードタスクが他のタスクの情報にアクセスしたり、システムの制御を獲得したりすることを防ぐことです。ESM は、各ユーザーモードタスクのアクセス範囲を制御することで、この仕組みを実現しています。

ESM の主な機能

アクセス制御ポリシー（ACP）：ACP により、各タスクが呼び出せる API を最小限に制限できます。タスクごとに使用可能な SAFERTOS® API 関数を明確に定義し、不要または危険な API 呼び出しを防止します。

オブジェクトアクセス制御ポリシー（OACP）：OACP を使用すると、各タスクがアクセス可能な SAFERTOS® のデータオブジェクト（タイマー、キュー、ミューテックス、セマフォ、イベントグループ、イベントプール、他タスクなど）を限定できます。タスクが他のタスクに属するデータ構造へ不正にアクセスすることを防ぎます。

データ難読化：重要なカーネルデータ構造は、メモリブロックへの直接ポインタではなく、間接参照を介してアクセスされます。悪意のあるコードによるデータ解析や改ざんを困難にします。

メモリ分離：ESM は、SAFERTOS® が提供する空間分離メカニズムを基盤とし、開発者がタスクごとに MPU/MMU のメモリ領域を定義できるようにします。各タスクは許可されたメモリ領域のみにアクセス可能であり、範囲外のアクセスが発生した場合は例外が発生します。

セキュア・ポータブルレイヤー：ESM を使用する場合、カーネル空間とユーザー空間をより厳格に分離する、セキュリティ対応のポータブルレイヤーが必要となります。

タスクコンテキストデータの分離：ESM では、タスクの実行コンテキストデータをタスクスタックではなく、TCB（Task Control Block）に格納します。待機中のタスクが他のタスクから不正に参照されることによる、情報漏洩や悪用を防止します。

侵入検出モニター：タスクが許可されていないメモリ、API、またはデータオブジェクトへアクセスした場合、例外が発生し、攻撃の可能性をアプリケーションに通知します。

DIOIZ
Enhance Your Embedded System

株式会社ディオイズジャパン
https://www.dioiz-japan.com
dioiz@dioiz.com、kmchoi@dioiz.com

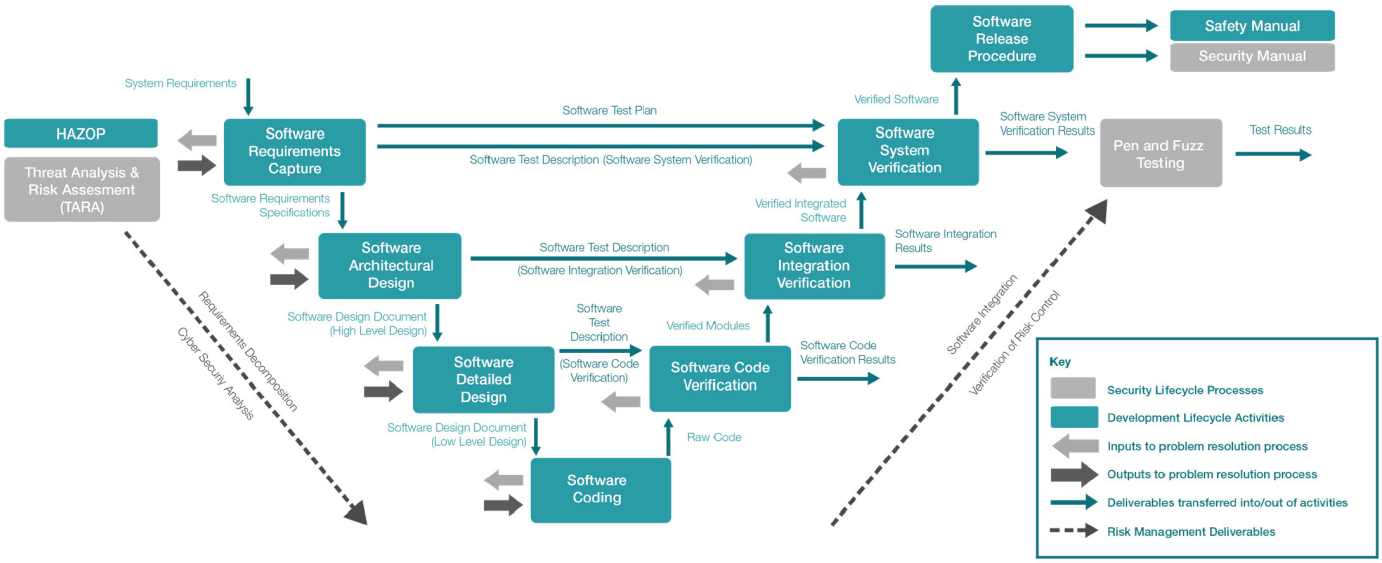

図 2. SAFERTOS® ESM 製品ライフサイクル

拡張セキュリティモジュール API

ESM が提供する機能は既存の SAFERTOS® API に影響を与えないため、既存プロジェクトへの導入が容易です。ただし、静的に定義されたオブジェクトやカーネルフック関数については、配置に注意が必要です。それぞれ KERNEL_DATA および KERNEL_FUNCTIONS に配置します。

さらに、スケジューラの初期化時にタスクのアクセス権限を設定できるよう、以下の API 関数が追加されています。

```
portBaseType xTaskConfigureACP(
    portTaskHandleType xTaskToConfigure,
    portUInt32Type ulTaskPermissionsMask,
    portUInt32Type ulTimerPermissionsMask,
    portUInt32Type ulQueueMutexSemaphorePermissionsMask,
    portUInt32Type ulEventpollEventGroupPermissionsMask
);
```

指定したタスクに対して、アクセス制御ポリシー（ACP）を設定します。この関数は、スケジューラの初期化状態にある場合のみ正常に実行されます。設定後は、タスクは権限マスクで許可された API 関数のみを使用でき、それ以外の API 呼び出しはエラーとなります。

```
portBaseType xTaskConfigureOACP(
    portTaskHandleType xTaskToConfigure,
    void *pvObjectToAllow
);
```

指定したタスクに対して、オブジェクトアクセス制御ポリシー（OACP）を設定します。
OACP により、タスクごとに特定の RTOS オブジェクトへのアクセス権を付与できます。スケジューラ起動前に xTaskConfigureOACP() を呼び出すことで、オブジェクトをタスクに割り当てます。
xTaskConfigureOACP() は、タスクのハンドル（xTaskToConfigure）と RTOS オブジェクトのハンドル（pvObjectToAllow）を指定して呼び出します。pvObjectToAllow に異なるオブジェクトを指定して本関数を複数回呼び出すことで、1 つのタスクに複数の RTOS オブジェクトへのアクセス権を付与できます。

開発プロセス

ESM は SAFERTOS® と同一の開発ライフサイクルを採用していますが、これに加えて追加のサイバーセキュリティ活動が含まれています。
安全要件の特定に用いられる従来の HAZOP に加え、WHIS では脅威分析およびリスク評価（TARA）ならびにサイバーセキュリティ分析レポート（CAR）を実施しています。サイバーセキュリティ要件は、既存の SAFERTOS® の機能要件および安全要件とともに、WHIS の要件管理ツールに登録されます。
すべての要件（安全性、機能性、サイバーセキュリティ）は、可能な限り高い安全整合性レベルで開発されます。
また、従来の機能検証および安全検証に加え、ペネトレーションテストおよびファズテストが開発ライフサイクルに組み込まれています。

DAP

SAFERTOS® ESM は、テストハーネスおよび SAFERTOS® API の使用例を含むデモンストレーションアプリケーションとともに、完全なソースコード形式で提供されます。
DAP には、特定のプロセッサ／コンパイラ構成向けに開発プロセスにおいて生成されたすべての設計および検証成果物が含まれており、安全およびサイバーセキュリティ関連ドキュメントならびにユーザーマニュアルも提供されます。

サポートおよびメンテナンス

年間契約に基づき、継続的なサポートおよびメンテナンスサービスを提供しています。
本サービスには、インシデントレポート、正誤表（エラッタ）通知、ならびに製品アップデートおよびパッチへのアクセスが含まれます。

評価版

評価版をご提供することが可能です。ご希望の場合は、お気軽にお問い合わせください。

DIOIZ
Enhance Your Embedded System

株式会社ディオイズジャパン
https://www.dioiz-japan.com
dioiz@dioiz.com、kmchoi@dioiz.com