参考資料

Application Note

TI のプロセッサを使用した堅牢な OTA システムの設計方法

Zekun Bai

概要

ワイヤレス (Over-the-Air、OTA) ファームウェア更新は、最新の組込みシステムにとって重要な機能であり、導入後に各種デバイスがソフトウェア更新を受信できるようにします。ただし、OTA プロセス中に問題が発生すると、デバイスが使用できなくなる可能性があります。

AM62 や他の Sitara™ プロセッサなどの TI プロセッサ ファミリは、強力なマルチコア アーキテクチャと豊富なペリフェラル インターフェイスを備えており、高い信頼性が求められる OTA アップデートを必要とする産業用および車載用アプリケーション向けに特化して設計されています。これらのプロセッサは、ARM® Cortex® R5/M4 コアと A53/A72 コアを内蔵し、各種メモリ インターフェイスとブート オプションをサポートしているほか、堅牢な OTA システムを構築するためのハードウェア基盤を実現します。

このアプリケーション ノートでは、TI のプロセッサを使用してより堅牢でフレキシブルな OTA システムを設計し、一般的な OTA 障害シナリオを回避する方法について説明します。

目次

商標

1 従来の OTA フローと分析

1.1 一般的な OTA 障害シナリオ

実際のアプリケーションでは、OTA アップデートによってシステムオンチップ (SoC) が動作不能になる可能性があります。分析を通じて、次のような一般的な問題があります。

- ブート メディアの電源レールが不安定なため、アプリケーションが破損する。
- バックアップ メカニズムがない。元のアプリケーションが破損すると、リカバリは不可能になる。
- アプリケーションのステータスおよびバージョン情報を示すステータス フラグがない。
- OTA より後の最初のブートを確認するための監視メカニズムがない。

1.2 従来の OTA プロセスの制限

従来の OTA (ワイヤレス) プロセスには、通常、ROM ブート、セカンダリ ブート ローダ (SBL)、およびアプリケーション バイナリが含まれます。更新すると、新しいアプリケーションは既存のアプリケーションを直接上書きしますが、堅牢性がありません。

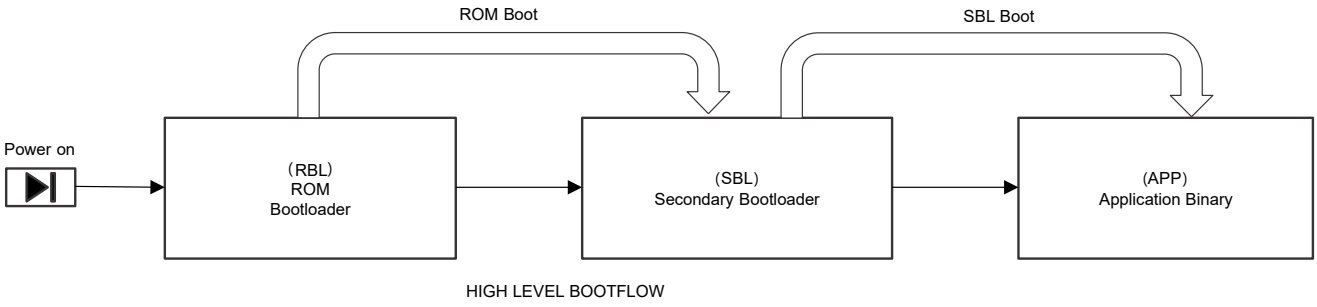

図 1-1. 従来のパワーオン スタートアップ プロセス

従来の OTA (ワイヤレス) アップデートには、電源をオンにしたときに、SD カードなどの新しいブート メディアを接続することが含まれます。SD カードには、アップグレードするアプリとブートローダー (SBL) が保存されます。ROM は SD カードからファイルをロードし、元のブート メディア上のアプリケーションの古い場所を上書きします。

このプロセスの主な問題は次のとおりです。

- バックアップ メカニズムがない：新しいアプリケーションが破損している場合、ロール バックする方法はありません。
- ステータス フラグがない：アプリケーションのステータスとバージョンを追跡できません。
- 監視メカニズムがない：OTA より後の最初のブートは監視できません。

2 TI プロセッサ OTA システムの革新的な設計

2.1 デュアル スロット設計により堅牢性が向上

TI のプロセッサは、以下のデュアル スロット設計をサポートしています。

- スロット A は元のアプリケーションを格納し、堅牢性を高めるために読み取り専用に設定されています。
- スロット B は OTA リクエストに使用され、新しいアプリケーションを格納します。
- この設計により、新しいアプリケーションが破損しても、システムは元のアプリケーションに戻すことができます。

2.2 ステータス フラグ システム

OTA ステータスを示すフラグ メカニズムが導入されています。

- フラグ = 0：SBL は、スロット A からアプリケーションをロードします。
- フラグ = 1：SBL は、スロット B から新しいアプリケーションをロードします。

お客様は、OTA の開始、OTA の進行中、OTA の完了など、より多くのフラグを定義することもできます。これにより、OTA プロセスがブラック ボックス化されるのを防ぐため、システムの OTA ステータスが外部に明確になります。

2.3 ロールバックのメカニズム

AB パーティショニング メカニズムに基づいて、WDG によってトリガされるコード ロールバック ロジックがチップのブート コアに追加されます。TI のプロセッサでサポートされているロールバック メカニズムは、主に以下の主要な要素によって実装されます。

1.ウォッチドッグ タイマの監視：

- SBL は、新しいアプリケーションのロード時にウォッチドッグ タイマを設定します。
- このタイマはセキュリティ対策として機能します。新しいアプリケーションが正しく動作しない場合、システム リセットがトリガされます。

2.アクノリッジ信号のメカニズム：

- 新しいアプリケーションが正常に開始した後、アクノリッジ信号 (ACK) を R5F-0 に送信する必要があります。
- アクノリッジ信号は、アプリケーションが初期化され、正常に動作していることを示します。
- アクノリッジを受信すると、R5F-0 はウォッチドッグ タイマをクリアし、更新プロセスを完了します。

3.フラグ ステータスの管理：

- システムは、現在のアプリケーションのロード位置を示すために永続フラグを使用します。
- フラグ = 0：スロット A から元のアプリケーションをロードします。
- フラグ = 1：スロット B から新しいアプリケーションをロードします。
- ロールバック中に、システムはフラグを 0 にリセットします。

4.自動ロールバック プロセス：

- 新しいアプリケーションがあらかじめ設定された時間内にアクノリッジ信号を送信しない場合：
- ウォッチドッグ タイマが満了し、システム リセットがトリガされます。
- システムはフラグを 0 に設定し直します。
- 再起動後、SBL はフラグ = 0 であることを検出し、スロット A から元のアプリケーションをロードします。

2.4 主要エリアの保護

ARM MPU (メモリ保護ユニット) は、メモリ領域のアクセス許可を構成することにより、ブートローダーを含むフラッシュ メモリを読み取り専用に設定します。これは、堅牢な OTA システムを設計する際の重要なセキュリティ対策です。

MPU によって、プロセッサは読み取り / 書き込み / 実行権限を含むメモリ領域の属性を定義できます。ブートローダーを保存するフラッシュ領域では、これを読み取り専用として構成でき、システムの実行中に他のプログラム (特にアプリケーション) がブートローダー コードを変更することを防止できます。

TI のプロセッサの OTA システム設計では、この保護メカニズムが特に重要です。分析によると、OTA 障害の一般的な原因は、新しいアプリケーションによるメモリの破損、特に SBL (セカンダリ ブートローダー) 領域の破損であり、これにより SoC が「動作不能」になることが判明しました。

NOR フラッシュ メモリの SBL ブートローダー領域を読み取り専用に設定することで、アプリケーションが誤ってまたは意図してこの重要なコードを変更することを効果的に防止できます。アプリケーションに問題が発生した場合でも、システムは正常なブートローダーを使用して回復できます。

これは、デュアル スロット設計、ステータス フラグ システム、ロールバック メカニズムとともに完全な保護システムを形成する、堅牢な OTA システムを設計するための重要なステップの一つです。

改善された NOR フラッシュ メモリのレイアウトには、デュアル バックアップ SBL (ブートローダー) とデュアル バックアップ アプリ (ビジネス ファイル) が含まれます。

表 2-1. NOR フラッシュ メモリのレイアウトを改善

NOR フラッシュ	ファイル
0xA	SBL ブートローダー
0xB	SBL ブートローダー
スロット A	アプリ A
スロット B	アプリ B

メモリの破損によってシステムが「動作不能」に変わることを防止するために、TI は MPU の重要な領域 (SBL など) に読み取り専用属性を設定することを推奨しています。

3 改善された OTA プロセス

TI のプロセッサを使用する堅牢な OTA プロセスには、以下のものが該当します。

1. 電源投入時に、SBL はフラグ (初期値 0) を確認し、アプリケーションをスロット A からロードします。
2. アプリケーションを実行し、OTA リクエストを確認します。
3. リクエストを受信すると、新しいアプリケーションがスロット B にロードされます。
4. フラグを 1 に設定し、リセットをトリガします。
5. SBL はフラグ (現在 1) を確認し、スロット B から新しいアプリケーションをロードします。
6. 新しいアプリケーションが実行されます。成功すると、アプリケーションは R5F-0 にアクノリッジを送信します。R5F はウォッチドッグ タイマをクリアし、更新を完了します。
7. ACK 確認がない場合、システムはロール バック (フラグが 0 に設定されている) し、スロット A から元のアプリケーションをロードします。

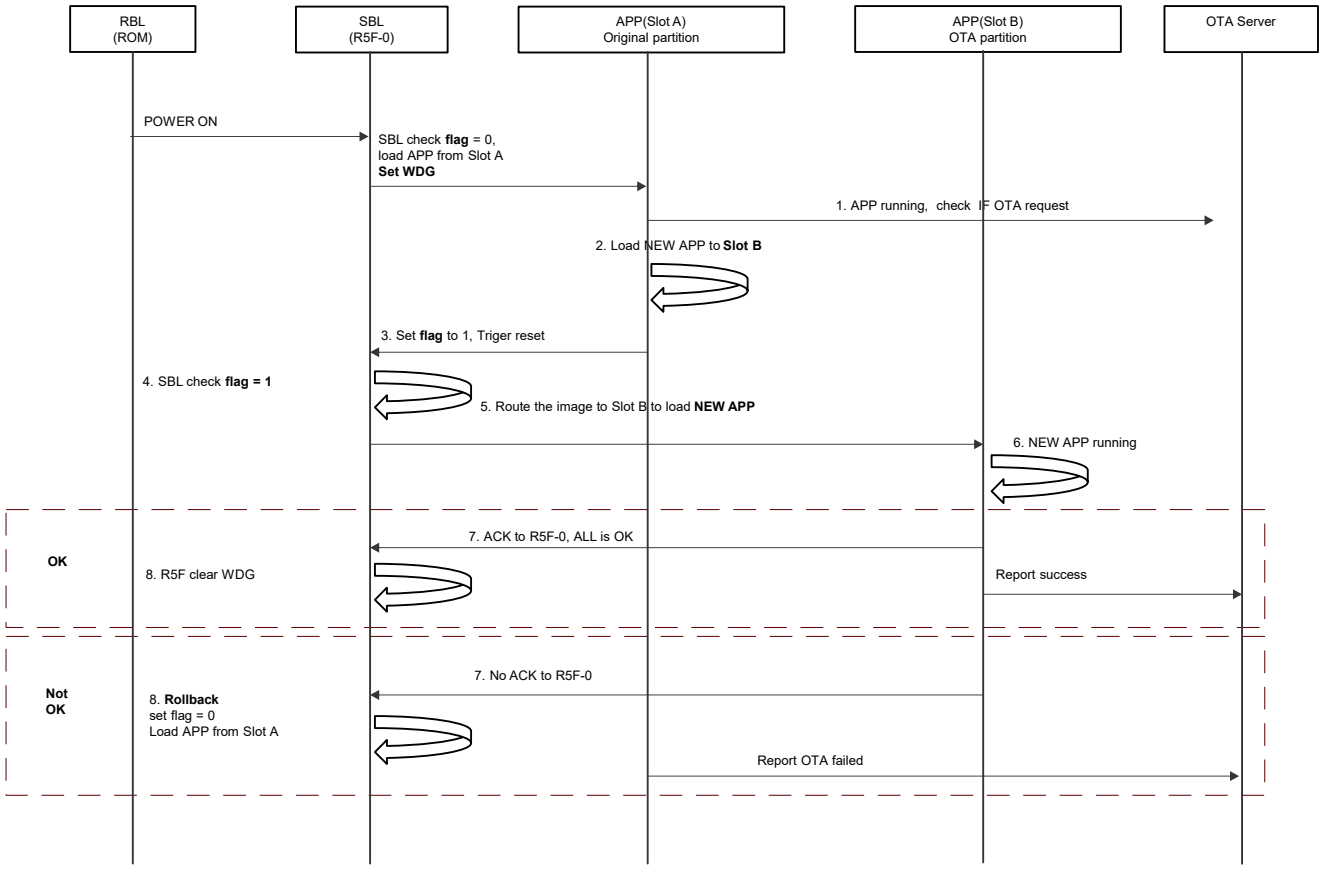

図 3-1. 改善された OTA フロー

4 まとめ

従来の OTA (ワイヤレス) アップデートでは、新しいアプリケーションが既存のアプリケーションを直接上書きするシンプルなメカニズムが採用されていました。そのため、重要なエリアのバックアップ メカニズム、ステータス フラグ、監視、保護がありません。アップデートが失敗すると、デバイスが使用できなくなる可能性があり、手動による介入が必要になります。

このホワイト ペーパーでは、ステータス フラグと自動ロールバック メカニズムを組み込んだデュアル スロット設計を用いた新しい OTA プロセスを提案し、アップデート失敗時のシステムの自動復旧を検証します。主な革新的技術には、デュアル スロット設計、ステータス フラグ システム、自動ロールバック メカニズム、および重要な領域の保護が含まれます。

この設計の複合的な利点として、システムの堅牢性の向上、保守のしやすさの向上、手動の介入不要、連続故障の防止、重要なシステム コンポーネントの保護を挙げることができます。

このホワイト ペーパーで提案している OTA システム設計方法は、AM62 プロセッサだけでなく、TI のの Jacinto™ プロセッサ ファミリ (車載インフォテインメントや ADAS アプリケーション用)、Sitara プロセッサ ファミリ (産業用オートメーションとエッジ コンピューティング デバイス用)、他の ARM ベースの TI プロセッサに拡張することもできます。

このフレキシブルで堅牢な OTA システム設計により、TI のプロセッサを使用したデバイスは、より信頼性の高いリモート更新機能を実現し、現場での保守コストの大幅な削減とエンド ユーザーの使いやすさの向上を可能にします。この設計アプローチは、信頼性の高い OTA 機能を必要とするさまざまな組込みシステムに適した重要なリファレンスとして活用できます。

5 参考資料

- テキサス インスツルメンツ、『AM62x Sitara™ プロセッサ』、データシート。

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、 TI の販売条件 、 TI の総合的な品質ガイドライン 、 ti.com または TI 製品などに関連して提供される他の適用条件に従い提供されます。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。 TI がカスタム、またはカスタマー仕様として明示的に指定していない限り、TI の製品は標準的なカタログに掲載される汎用機器です。

お客様がいかなる追加条項または代替条項を提案する場合も、TI はそれらに異議を唱え、拒否します。

最終更新日：2025 年 10 月