Application Note

How to Design Robust OTA System using TI Processors

Zekun Bai

ABSTRACT

Over-the-Air (OTA) firmware updates are a critical function of modern embedded systems, allowing devices to receive software updates after deployment. However, any issues during the OTA process can render a device unusable.

TI processor families, such as the AM62 and other Sitara™ processors, offer powerful multi-core architectures and rich peripheral interfaces, making them particularly designed for industrial and automotive applications requiring highly reliable OTA updates. These processors integrate an ARM® Cortex® R5/M4 core and A53/A72 cores, supporting various memory interfaces and boot options, providing the hardware foundation for robust OTA systems.

This application note describes how to use TI processors to design more robust and flexible OTA systems, avoiding common OTA failure scenarios.

Table of Contents

Trademarks

1 Traditional OTA Flow and Analysis

1.1 Typical OTA Failure Scenarios

In practical applications, OTA updates can turn the System-on-Chips (SoC) into brick. Through analysis, these are the following common issues:

- Unstable power rails on the boot media cause application corruption.
- Lack of backup mechanism; once the original application is corrupted, recovery is impossible.
- No status flags indicate application status and version information.
- Lack of monitoring mechanism to check the first boot after OTA.

1.2 Limitations of Traditional OTA Processes

Traditional OTA (Over-The-Air) processes typically involve ROM booting, a secondary boot loader (SBL), and application binaries. When updating, the new application directly overwrites the existing one, which lacks robustness.

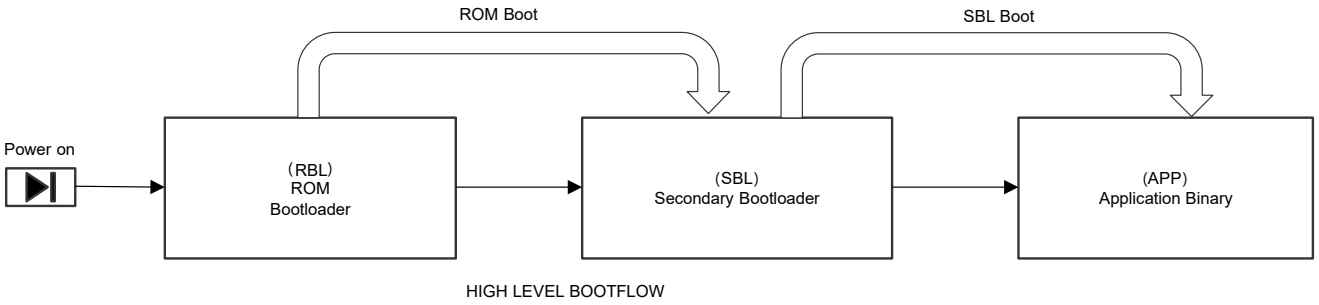

Figure 1-1. Traditional Power-On Startup Process

Traditional OTA (Over-The-Air) updates involve connecting a new boot medium, such as an SD card, during power-on. The SD card stores the app to be upgraded and the bootloader (SBL). The ROM loads the files from the SD card, overwriting the old location of the application on the original boot medium.

The main problems with this process are:

- No backup mechanism: If the new application is corrupted, there is no way to roll back.
- No state flags: Application status and version cannot be tracked.
- No monitoring mechanism: The first boot after OTA cannot be monitored.

2 Innovative Design of TI Processor OTA System

2.1 Dual-Slot Design Enhances Robustness

TI processors support a dual-slot design:

- Slot A stores the original application and is set to read-only for increased robustness.
- Slot B is used for OTA requests and stores new applications.
- This design makes sure that even if a new application is corrupted, the system can still revert to the original application.

2.2 Status Flag System

A flag mechanism is introduced to indicate OTA status:

- Flag = 0: SBL loads the application from slot A.
- Flag = 1: SBL loads the new application from slot B.

Customers can also define more flags, such as those representing OTA start, OTA in progress, and OTA complete. This makes the OTA status of the system clearer to the outside world, preventing the OTA process from becoming a black box.

2.3 Roll-Back Mechanism

Building upon the AB partitioning mechanism, a code rollback logic is added to the boot core of the chip, triggered by WDG. The rollback mechanism supported by TI processors is primarily implemented through the following key elements.

1. Watchdog Timer Monitoring:

- SBL sets a watchdog timer when loading a new application.
- This timer serves as a security measure; if the new application fails to run properly, this triggers a system reset.

2. Acknowledgment Signal Mechanism:

- After a new application successfully starts, acknowledgment signal must be sent (ACK) to R5F-0.
- The acknowledgment signal indicates that the application has been initialized and is running normally.
- Upon receiving the acknowledgment, R5F-0 clears the watchdog timer, completing the update process.

3. Flag State Management:

- The system uses persistent flags to indicate the current application loading position.
- Flag = 0: Load the original application from slot A.
- Flag = 1: Load the new application from slot B.
- During rollback, the system resets the flag to 0.

4. Automatic Rollback Process:

- If the new application does not send an acknowledgment signal within the predetermined time:
- The watchdog timer expires, triggering a system reset.
- The system sets the flag back to 0.
- After restarting, SBL detects that flag = 0 and loads the original application from slot A.

2.4 Key Area Protection

The ARM MPU (Memory Protection Unit) sets the flash memory containing the bootloader to read-only by configuring access permissions for the memory region. This is a critical security measure when designing robust OTA systems.

The MPU allows the processor to define the attributes of memory regions, including read/write/execute permissions. For the flash region storing the bootloader, this can be configured as read-only, preventing other programs (especially applications) from modifying the bootloader code while the system is running.

This protection mechanism is particularly important in the OTA system design of TI processors. Analysis shows that a common cause of OTA failure is memory corruption by new applications, especially corruption of the SBL (Secondary Bootloader) region, rendering the SoC *bricked*.

By setting the SBL bootloader region in NOR flash memory to read-only, this effectively prevents applications from accidentally or maliciously modifying this critical code. Even if the application has problems, the system can still recover using a healthy bootloader.

This is one of the important steps in designing a robust OTA system, forming a complete protection system along with dual-slot design, status flag system, and rollback mechanism.

The improved NOR flash memory layout includes: dual-backup SBL (Bootloader) and dual-backup APP (business files).

Table 2-1. Improved NOR Flash Memory Layout

Nor Flash	Files
0xA	SBL Bootloader
0xB	SBL Bootloader
Slot A	APP A
Slot B	APP B

To prevent memory corruption from turning the system into a *brick*, TI recommends setting read-only attributes for critical areas (such as SBL) in the MPU.

3 Improved OTA Process

The robust OTA process using a TI processor includes:

1. Upon power-up, the SBL checks the flag (initially 0) and loads the application from slot A.
2. Runs the application and checks for OTA requests.
3. If a request is received, loads the new application into slot B.
4. Sets the flag to 1 and triggers a reset.
5. The SBL checks the flag (now 1) and loads the new application from slot B.
6. The new application runs; if successful, the application sends an acknowledgment to R5F-0. R5F clears the watchdog timer, completing the update.
7. Without ACK confirmation, the system rolls back (flag set to 0) and loads the original application from slot A.

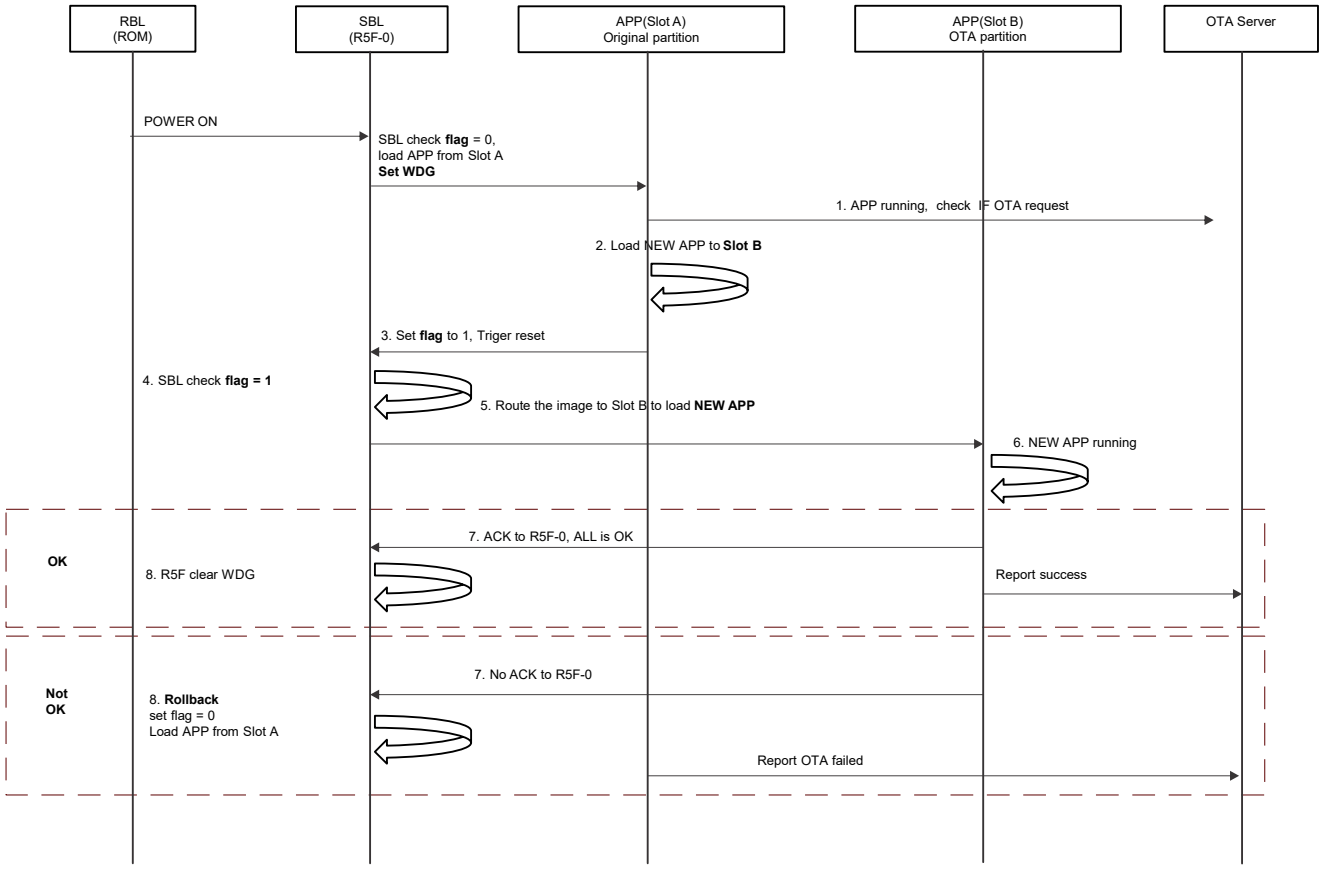

Figure 3-1. Improved OTA Flow

4 Summary

Traditional OTA (Over-The-Air) updates employ a simple mechanism where new applications directly overwrite existing ones. This lacks backup mechanisms, status flags, monitoring, and protection for critical areas. If an update fails, the device can become unusable, requiring manual intervention.

This paper proposes a novel OTA process using a dual-slot design, incorporating status flags and an automatic rollback mechanism to verify automatic system recovery in the event of update failure. Key innovations include: dual-slot design, status flag system, automatic rollback mechanism, and protection of critical areas.

The combined advantages of this design include: enhanced system robustness, improved maintainability, no manual intervention required, prevention of consecutive failures, and protection of critical system components.

The OTA system design method proposed in this paper is not only applicable to AM62 processors but can also be extended to TI's Jacinto™ processor family (for automotive infotainment and ADAS applications), Sitara processor family (for industrial automation and edge computing devices), and other ARM-based TI processors.

Through this flexible and robust OTA system design, devices using TI processors can achieve more reliable remote update capabilities, significantly reducing field maintenance costs and improving the end-user experience. This design approach provides a valuable reference for various embedded systems that require high-reliability OTA functionality.

5 References

- Texas Instruments, AM62x Sitara™ Processors, datasheet.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025