ANALOG DEVICES

AN-1263
APPLICATION NOTE

One Technology Way • P.O. Box 9106 • Norwood, MA 02062-9106, U.S.A. • Tel: 781.329.4700 • Fax: 781.461.3113 • www.analog.com

Security Integrity of the ADuCM350

INTRODUCTION

The ADuCM350 offers various features developed to address the following three goals:

- To ensure that the device conditions are suitable for code execution
- To prevent unauthorized access or copying of user code
- To prevent tampering of a device with the intention of altering its intended use

This application note outlines the initialization, real-time checking, authentication, flash, JTAG/serial wire, failure analysis, and serial downloader features.

INITIALIZATION

Power supply monitors ensure that the device is properly powered and do not allow execution outside an acceptable range. Monitoring is continuous.

Flash hardware performs a CRC32 signature check of all flash information space memory (factory installed kernel) before the first instruction fetch is performed. This validates that the flash can be reliably accessed.

Upon completion of kernel execution, a CRC32 signature check of user Page 0 is performed before the first user instruction is performed.

- Signature check is performed using forward signature only.
- During development, the check can be skipped if the signature written to flash (Address 0x7FC) is 0xFFFFFFFF.

REAL-TIME CHECKING

Word parity checking on each flash access can be performed to prevent code execution in the event of an intermittent bit failure. Itmonitors and detects, but does not make corrections.

Under user control, forward and backward hardware accelerated CRC32 signature checking across any number of pages can be performed, as an interval check, during run time.

An integrated watchdog timer monitors real-time operation or monitors the part in hibernate mode.

AUTHENTICATION

A truly random number generator implemented in the hardware allows the formulation of challenge responses.

An optional elf hash calculation across instruction space can be performed and stored within flash. During user code execution, a hash function can be called to authenticate flash user code (this complements the CRC signature check feature).

FLASH

Write protection of individual pages can be programmed to prevent accidental overprograming of flash memory.

In general, all flash commands are key protected to avoid accidental flash operations, such as program, erase, and so on.

JTAG/SERIAL WIRE

As a feature, JTAG/serial wire access is user controlled, preventing debug access and viewing of user code.

- On power up, JTAG/serial wire access is disabled if a control key has been programmed by the user in the reserved space of user flash (Address 0x5FFE8). Otherwise, the JTAG/serial wire access is enabled. The value of the control key is 0x16032010.
- Additionally, JTAG/serial wire access can be enabled/disabled in the application code by writing to the FEECON1 register.

FAILURE ANALYSIS

Analog Devices, Inc., has access to the device for failure analysis, but cannot view customer code without the assistance of the customer.

Failure analysis of flash-related issues can only be accomplished in cooperation with the customer (a user-specified key must be supplied to Analog Devices).

SERIAL DOWNLOADER

Using the UART interface, a part can be bulk erased and reprogrammed. This is useful in the event a part is improperly programmed, such as if the debug access is locked out.

For bulk erase, there must be access to a pin dedicated to this purpose. This allows the customer to protect access to the downloader pin.

The serial downloader does not have read capability, thus user code is protected.

NOTES

REVISION HISTORY

11/13—Revision 0: Initial Version