winbond

RZ Ecosystem Partner Solution

Winbond Boot Code Integrity Protection and Firmware Resilience

Solution Summary

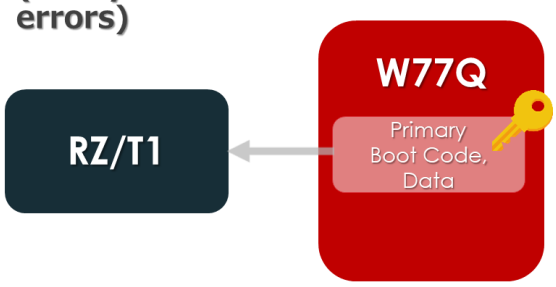
Winbond secure flash W77Q provids 'add-on' security in the boot code integrity and firmware resilience on RZ/T1 platform.

Features/Benefits

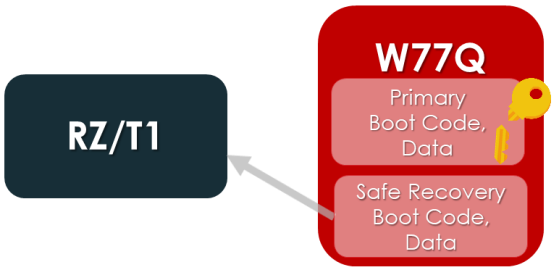
- W77Q secure flash memory is compatible to standard SPI NOR flash memory.
- W77Q can be "Root-Of-Trust" for ROM-Less SoC.
  - W77Q automatically verifies boot code by itself and raises reset pin from "L" to "H" for SoC.
  - If the boot code was hacked, W77Q automatically jump to redundant boot code for recovery.
- Platform Firmware Resilience supported
  - Referenced to NIST SP800-193

Diagrams/Graphics

Self Integrity Protection (Verify Boot Code to detect errors)



Safe Fallback = Firmware Resilience (Recovery)



☐ Self Integrity Protection

- ➢ Primary Boot Code shall be verified from falsification or errors
- ➢ After passed the verification, SoC can start fetching (Secure Boot)
- ➢ Two control methods for SoC to wait; A H/W pin (RSTOUT#) or S/W loop

☐ Safe Fallback

- ➢ If primary Boot Code had problem, switch to other redundant Boot Code for recovery automatically

Target Markets and Applications

- Network, IoT
- Industries requiring security guideline
  - ISO/IEC62443-4-2
  - CC/EAL, GP/SESIP, ASIL certification

https://www.winbond.com/hq/?__locale=en

2021.09

winbond

A trusted supplier of advanced memory products

From R&D through advanced manufacturing to dedicated customer service, Winbond Electronics Corporation is a total memory solutions provider.

Winbond's product portfolio consists of specialty DRAM, mobile DRAM, code storage Flash memory, and TrustME® secure Flash memory products. The company serves customers in the communications, consumer electronics, automotive, industrial, and computer peripherals markets, supplying its products directly or via a global network of authorized distributors.

Winbond's headquarters are in the Central Taiwan Science Park, and it operates wafer fabrication plants in Taichung and Kaohsiung in Taiwan. Subsidiaries in the USA, Japan, Israel, China and Hong Kong perform marketing operations and provide direct support to customers.

Winbond's combination of advanced semiconductor technologies developed in-house and close relationships with customers support its position as a trusted supplier of memory products.

Company Name	Winbond Electronics Corporation
Date of Establishment	1987-09-29
Chairman	Arthur Yu-Cheng Chiao
Vice Chairman	Thung-Yi Chan
President	Pei-Ming Chen
Capital Stock	39.8 billion Taiwan dollars (as of October 2020)
Number of employees	3048 (as of October 2020)
Headquarters Location	No. 8, Keya 1st Rd.,Daya Dist.,Central Taiwan Science Park, Taichung City 42881, Taiwan
Overseas Branches	USA, Japan, Israel, China, Hong Kong, Germany