BCM63XX

FAILSAFE BOOT

Application Note

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

1 Description

Beginning with release 5.02L.07, FAILSAFE_BOOT is supported on devices that use GEN3 Secure boot ROM boot. When enabled, the standard Linux watchdog must also be configured.

The FAILSAFE boot mechanism allows a watchdog to reboot to a previously programmed image in the event that the system becomes unresponsive during the boot process. This mode only works on types of failure which are recoverable via SoftReset.

The implementation enables CFEROM, CFERAM, and Linux Userspace to maintain a run-time (RT) state across the software stack via storing the state in SoftReset-safe register. The WATCHDOG (WD) is enabled in specific places within the bootloaders where significant boot stages can be identified.

An RT state is a combination of the following values (state | error):

- state is one of CFE_BOOT_INFO_ROM, CFE_BOOT_INFO_PRIMARY, CFE_BOOT_INFO_SECONDARY, CFE_BOOT_INFO_LINUX.
- error is one of CFE_BOOT_ERR_OK, CFE_BOOT_ERR_ABORTED, CFE_BOOT_ERR_CRIT.

These stages/points are:

CFEROM

1. On init, before DDR initialization, process state to make decision, as in the following:

   If booted from PoR or if error is CFE_BOOT_ERR_OK:

   – Set state CFE_BOOT_INFO_ROM and set error CFE_BOOT_ERR_ABORTED.

     WD armed unconditionally.

   If booted from SoftReset:

   If state = CFE_BOOT_INFO_ROM and err = CFE_BOOT_ERR_ABORTED:

   - Select DDR safe mode

   Else, if state = CFE_BOOT_INFO_PRIMARY and err = CFE_BOOT_ERR_ABORTED:

   - Set state to CFE_BOOT_INFO_SECONDARY and err to CFE_BOOT_ERR_CRIT.

     If state also had CFE_BOOT_INFO_LINUX value, then it is added to the state accordingly, for example, state set to CFE_BOOT_INFO_SECONDARY|CFE_BOOT_INFO_LINUX.
   - Select to boot from other (inactive) image on flash.

   Else, if state = CFE_BOOT_INFO_SECONDARY and err = CFE_BOOT_ERR_CRIT:

   - CFEROM halts without return.

   Arm watchdog.

2. Before loading/starting CFERAM from flash image from the storage such as SPINAND/NAND/EMMC:

   If state = CFE_BOOT_INFO_ROM:

   – Set state to CFE_BOOT_INFO_PRIMARY.

   Arm watchdog.

   – Boot to the selected image.

CFERAM

1. Init stage:
   – Arm watchdog (to avoid expiration of timer).
2. Before Linux loading:

   If state = CFE_BOOT_INFO_PRIMARY of CFE_BOOT_INFO_SECONDARY:
   - Add to state CFE_BOOT_INFO_LINUX.
   - Arm watchdog.

     If user pressed key to drop to console, stop state tracking; disable WD.

Linux User Space

- On init script S1, re-arm watchdog.
- On init script S89, stop watchdog, set RT error to CFE_BOOT_ERR_OK. (This value should still be present whenever Linux does an intentional reboot.)

Every time WD is armed the default counter is set to expire in 30s. If not reset or disabled, WD will soft-reset SoC. On every stage as described above, WD is disarmed as required to update the RT state then re-armed to continue to the next tracked stage.

The RT state is accessible via proc kernel entry.

/proc/boot/failsafe -

Reading this entry would return the following values:

- ACTIVE: indicating normal boot.
- PREVIOUS: indicating that booted image was an attempt to recover from crash or stall during the boot of the ACTIVE image.

Writing 0 to it resets an error status to success.

NOTE: There is no built-in functionality to make policy decisions to either continue attempting to use the failed image, invalidating, or performing an upgrade. Customer-specific code can base policy decisions on /proc/boot/failsafe or use other means to reset the watchdog.

Revision History

BCM63xx FAILSAFE BOOT NOTE-R, July 10, 2019

- Initial release