

HARDWARE ASSISTED FAULT INJECTION DETECTION

ABSTRACT

Anti-fault injection systems and methods are disclosed. An anti-fault injection system includes a processor; a boot ROM configured to store a series of boot instructions executable by the processor; and anti-fault injection controller circuitry. The anti-fault injection controller circuitry is accessible to the processor while the processor is executing the boot instructions. The anti-fault injection controller circuitry includes interrupt/reset circuitry configured to interrupt the processor in response to a trigger and secure boot circuitry. The secure boot circuitry is configured to, in response to being accessed by the processor: determine whether the processor is executing non-secure boot instructions in error; and in response to detecting that the processor is executing non-secure boot instructions in error, provide the trigger to the interrupt/reset circuitry.

Fig. 3A