3 RESET HIERARCHY

Some applications require a robust system that is not affected by the failure of other systems. For example, even if the main cluster or sub-cluster system hangs and is reset, the SIC system is required to operate properly. To support the robust system, TCC807x provides various types of resets.

Figure 3.1 shows four types of resets and the reset sources of each reset in the Normal Boot with SIC boot sequence. Each reset has different scopes.

Note: In the Normal Boot without SIC boot sequence, the SIC sub-system is not available.

According to the configuration, the safety-related blocks are set to be selectively reset by cold reset or AP system reset. For example, when reset for SDM is masked, SDM is not reset even if cold reset occurs.

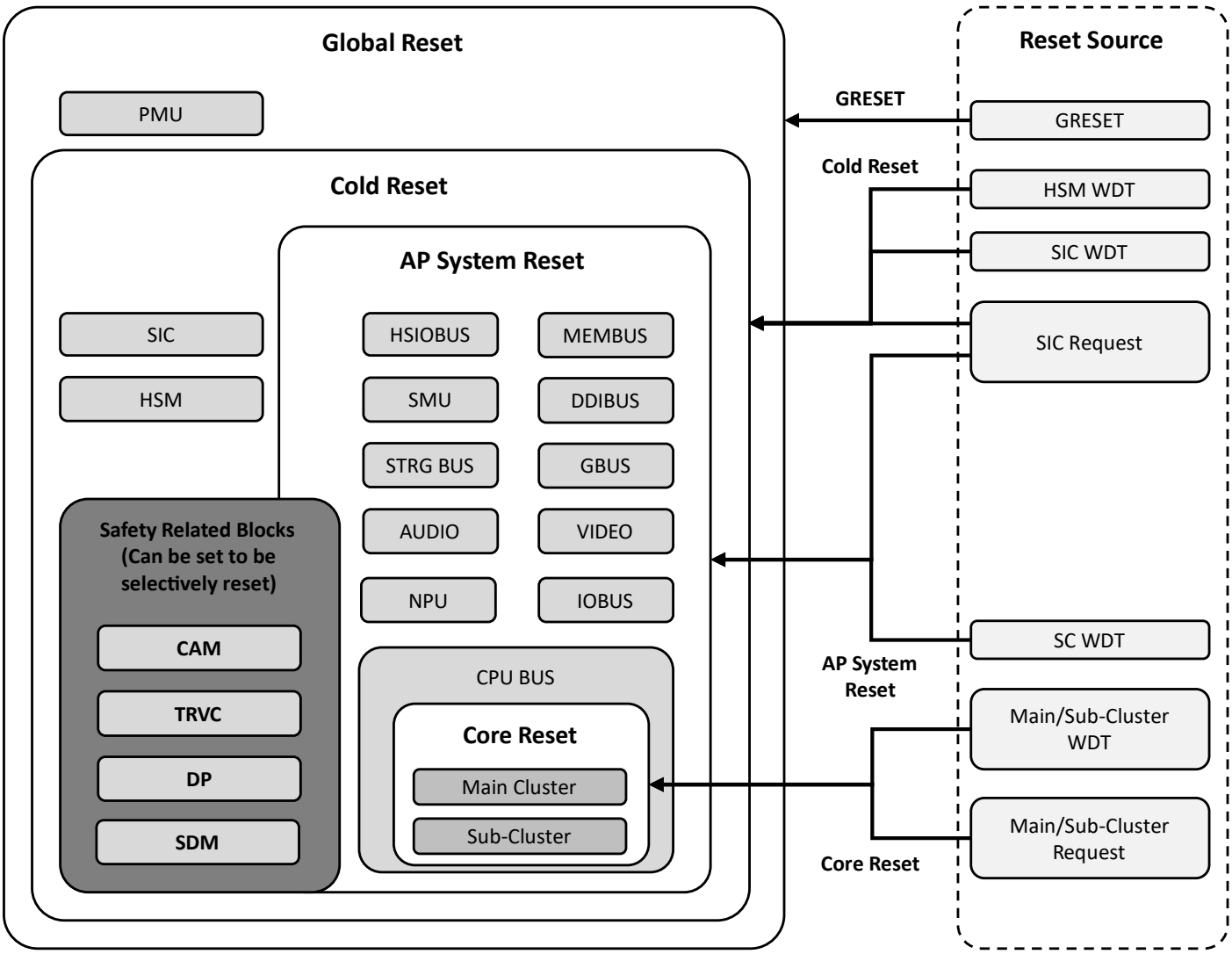

Figure 3.1 Block Diagram of TCC807x Reset (Normal Boot with SIC)

Table 3.1 describes the processor that performs the reset and the reset sources of each reset in BMs (Normal Boot with SIC and Normal Boot without SIC).

In Normal Boot with SIC:

- Cold reset occurs when SIC or HSM watchdog reset occurs or is executed by SIC on its request.
- AP system reset is executed by SIC when SC watchdog reset occurs, or on its request.
- Core reset of main cluster or sub-cluster is executed by SC when main cluster or sub-cluster watchdog reset occurs, or on main cluster or sub-cluster's request.

In Normal Boot without SIC:

- Cold reset occurs when SC or HSM watchdog reset occurs.
- AP system reset is not used.
- Core reset of main cluster or sub-cluster is executed by SC when main cluster or sub-cluster watchdog reset occurs, or on main cluster or sub-cluster's request.

Table 3.1 Processor and Reset Source of TCC807x Reset

<table>
<tr><th rowspan="2">Reset</th><th colspan="2">Normal Boot with SIC</th><th colspan="2">Normal Boot without SIC</th></tr>
<tr><th>Processor</th><th>Reset Source</th><th>Processor</th><th>Reset Source</th></tr>
<tr><td>GRESET</td><td>N/A</td><td>GRESET</td><td>N/A</td><td>GRESET</td></tr>
<tr><td rowspan="2">Cold Reset</td><td>N/A</td><td>SIC Watchdog Reset
HSM Watchdog Reset</td><td rowspan="2">N/A</td><td rowspan="2">SC Watchdog Reset
HSM Watchdog Reset</td></tr>
<tr><td>SIC</td><td>SIC Request</td></tr>
<tr><td>AP System Reset</td><td>SIC</td><td>SC Watchdog Reset
SIC Request</td><td colspan="2">Not used</td></tr>
<tr><td>Core Reset</td><td>SC</td><td>Main/Sub-cluster Watchdog Reset
Main/Sub-cluster Request</td><td>SC</td><td>Main/Sub-cluster Watchdog Reset
Main/Sub-cluster Request</td></tr>
</table>

4 REDUNDANT BOOT

TCC807x has two identical sets of boot images, the primary images and the secondary images, to support redundant boot. When TCC807x fails to boot with primary images, it retries booting with the secondary images. When TCC807x fails to boot with secondary images, it enters firmware download mode.

Figure 4.1 shows the flowchart of TCC807x redundant boot.

At each boot level, the processors can recognize the boot failure status by checking Boot Failure Flag (BFF). By checking BFF, the processors can determine which boot images to use (primary images or secondary images). If BFF indicates that boot is failed for both images, TCC807x enters firmware download mode. If image loading or verification fails, it is considered as the boot failure and the processor sets BFF and operates reset.

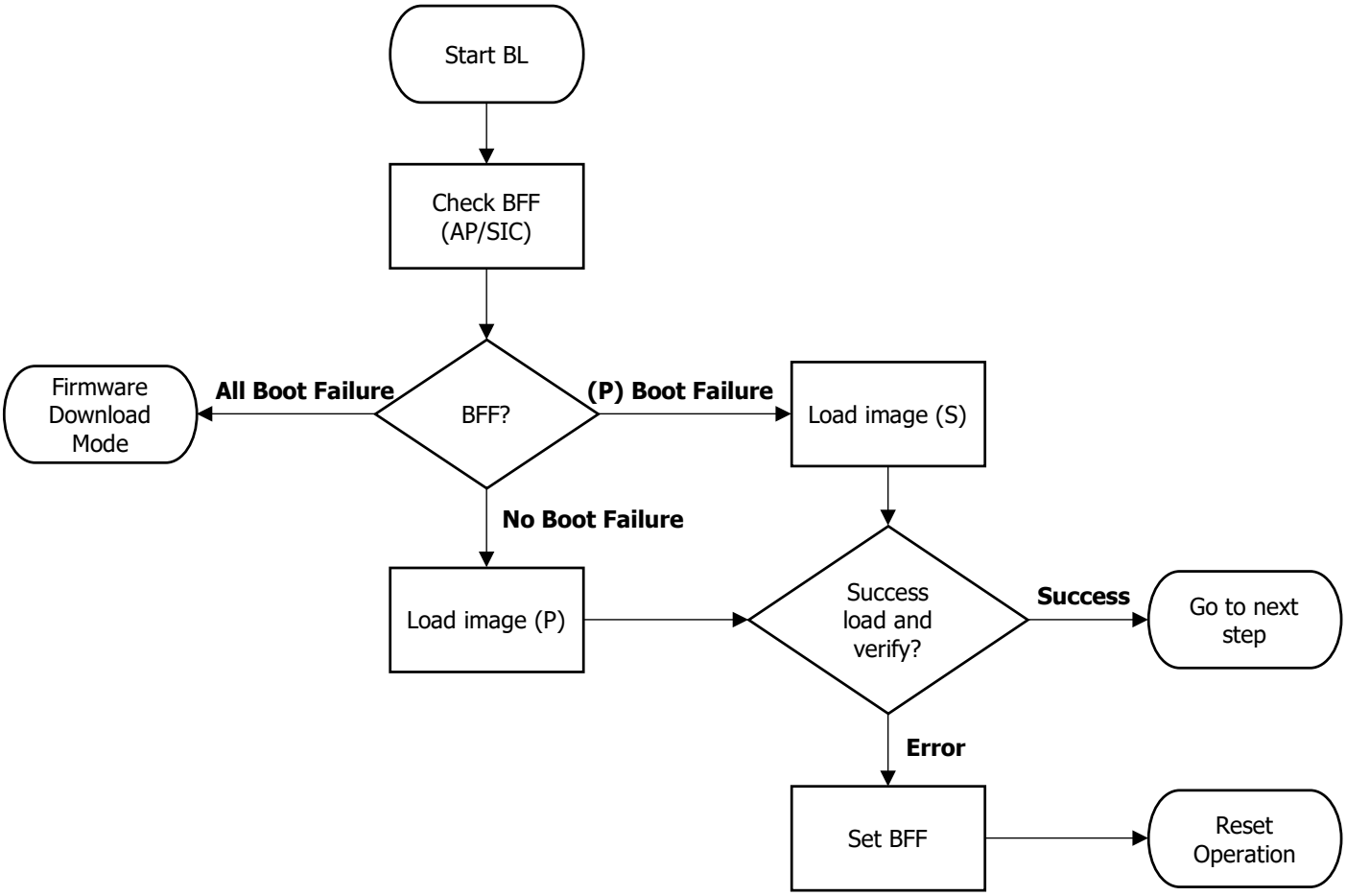

Figure 4.1 Flowchart of TCC807x Redundant Boot