Safe Power-down Mechanisms for Digital Processors

Contributed by Nabeel Shah and Shivakumar Puran and Shivakumar Puran *Rev 01 – September 5, 2023*

Introduction

Sudden power failure or power loss in a system-on-chip (SoC) can lead to unpredictable behavior, especially when the SoC is actively running software and using I/O peripherals. Power loss can result in unexpected states on the pins of the SoC. Because the power to the SoC internal logic is no longer within operational range and is unable to drive the pins to known state. This can potentially cause issues when other system components expect certain pins in a specific state. The system design can mitigate the chances of the proper malfunction under such conditions.

This application note discusses a way to address this problem. The core idea is based on the concept of having the capability to detect a power failure as early as possible and to implement a safe SoC shutdown sequence to protect system components and data. One effective approach uses a voltage monitor circuit to detect when the power supply voltage falls below a certain threshold, which can then trigger the safe shutdown sequence. By taking these measures, system designers can minimize the potential risks associated with sudden power failure in SoCs and ensure reliable and consistent operation of their system.

Applicable Processors

The processor series for this EE Note includes these products:

- ADSP-SC58x/ADSP-2158x
- ADSP-SC57x/ADSP-2157
- ADSP-2156x - has OSPI controller
- ADSP-2159x/ADSP-SC591/SC592/SC594 - has OSPI controller
- ADSP-SC595/SC596/SC598 - has OSPI controller

Take Aways

The analysis clearly shows that using a power failure detection circuit is useful for implementing a reliable and safe power down. This method avoids some of the indeterminacy issues and unexpected operations that can otherwise happen during an unplanned power down.

In a customer system, when a similar provision is made to ensure the source power supply is monitored and the system reset is issued before the SoC power rails start to decrease. That prevents the SoC from continuing to operate during a power down and it enters a deterministic reset state long before the SoC power domains start decreasing.

SoC Power Down

This section discusses power down impact on a series of SHARC-based DSPs from Analog Devices. During a power-down sequence, as different power rails collapse and decrease below minimum operating specification (See the first five product datasheets [1][2][3][4][5] found in References), the processor cannot operate reliably and deterministically. One of the unreliability consequences is that the processor output pins can have indeterministic state and may not be able to drive the known state (for example, tri-state). During a power down, when VDD_INT drops below minimum specifications (for example, 0.95V for the ADSP-SC594 processor), the effect undetermined, because the chip is operating outside its designed specifications. When any part of the chip logic decreases to this voltage range(that is, below the VDD_INT minimum specification) the behavior of that logic, whether it is the cores or any peripheral, cannot be determined.

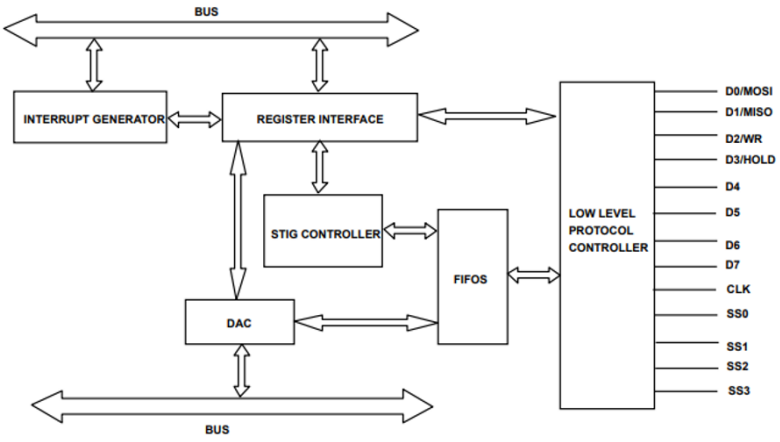
When VDD_EXT (and VDD_REF) operate within specifications, plus the VDD_INT drops below the minimum specification, indeterminate logic operations can result in an indeterminate state or switching on I/O pins. Only when the VDD_INT approximates 0V, can the VDD_INT supply be defined as *Off*. It is at this low voltage when the VDD_INT logic cannot impact any I/O operations. When VDD_INT drops below minimum operating conditions, there is no internal monitoring circuit in the chip to react and stop the core execution. The core continues the execution (with unknown behavior) even when the voltage drops below the minimum operating level.

Note: Indeterminate pin states during the power down is an expected behavior as these processors are not designed to be safety compliant especially for sudden power down. And thus, the behavior during power down is not deterministic.

OSPI During Power Down

As listed in the Applicable Processors section, some processors have an OSPI controller to help the processor interface with different NOR flash devices. The OSPI controller supports memory-mapped read and write operations that allows the OSPI controller to convert the AXI read/write transactions (by system masters like Core and MDMA) into low-level SPI bus transactions. These permit the OSPI controller to read to or write from the flash devices. This operation mode is called *Direct Access Controller* mode. More details about this mode can be found in the OSPI chapter of processor hardware reference manuals HRM under the title *Direct Access Controller (DAC)*.

Figure 1: Direct Access Controller Block Diagram



When an enabled OSPI controller has DAC mode set, there can be read or write accesses started on OSPI pins when the SoC powers down. These read and writes accesses can be started regardless of whether any software accesses the OSPI interface or not. Read accesses are of no concern because they are non-destructive. However, write accesses pose a risk of corrupting the flash memory contents when the address of the write command points to a flash address containing valid data.

Unlike other peripherals and pad pins which can have an indeterminate state during the power down, the OSPI controller (DAC mode is enabled) can drive known commands on the OSPI pins during the power down. This is because the DAC engine is a hardware state machine, capable of automatic sequence SPI command generation. Any random trigger of an OSPI block due to non-specification voltage in core voltage domain, can launch a valid flash access on outside pins, which can trigger the flash to start a read or write operation.

SPI During Power Down

Like the OSPI controller, an SPI controller also supports memory-mapped read operation. The possibility of an SPI controller generating read accesses to flash during the power down can happen. This can happen when an SPI controller is enabled with memory-mapped mode and chip is powered down. However, because an SPI supports only memory-mapped read operations, there is no possibility of write access from an SPI to the flash device.

Possible Mitigations

The GPIO pins have an expected indeterminate state during a power down and must be addressed as part of the system-level design to ensure that rest of the SoC remains unaffected. Moreover, the GPIO can have random states during the power down and are not able to create any meaningful outside operations.

However, with the OSPI controller, there is a possibility of generating valid read/write operations during the power down when the controller DAC mode is enabled. Then write operations can result in flash memory corruption. This can corrupt the critical user data in the flash which can affect the application software on a subsequent boot up. Worse, it can corrupt the boot image in the flash that cause the boot failure on next power-up cycle.

To avoid that scenario, there are software actions an engineer can take. Some of these actions are:

- Disable the DAC mode of the OSPI controller.
- Program invalid opcodes (WEN command and WRITE command) for write operations in DAC mode.
- Enable the write protection in the OSPI controller.
- Enable SMPU protection for disabling write accesses to OSPI controller.

Some of these measures are not always possible, especially when the user application does write accesses to the flash. To overcome this limitation in a reliable way, an engineer can implement power failure detection techniques, as discussed in the General Power Failure Detection section.

General Power Failure Detection

Power failure detection determines the loss of the electrical power supply to a system or device. Power failure can happen because of different reasons, such as a blackout, a blown fuse, a tripped circuit breaker, drained battery, or a fault in the power supply system. The detection of a power failure can be implemented using several technologies, such as sensors that detect changes in voltage or current. For the power failure detection to be useful in reliably shutting down the SoC, there must be sufficient time between power failure detection and the time when voltage rails powering the SoC decrease below minimum specifications. The warning time ($t_{warning}$, or the interval between failure detection and decreased voltage on rails) must be sufficient to permit the system to invoke and complete the procedures to put the SoC in safe state. Unless the software can start sequences to disable peripherals or put the entire SoC in reset, the power failure detection is not very useful.

Because there are multiple power rails to power the SoC, the power supply design is hierarchical; making use of multiple buck power regulators to generate all the SoC power rails. Usually, system design uses 12V or 5V as the input power supply to derive different power rails for the SoC and other board components. This inevitably results in a delay between the decrease on the SoC power rail and the decreased input power supply. The delay depends on the power consumption of multiple power rails, which are sourced by the input power supply. With more power consumption, comes a faster power supplies collapse. However, there is a delay ($t_{warning}$) between master power supply stops and the time when downstream power supplies stop.

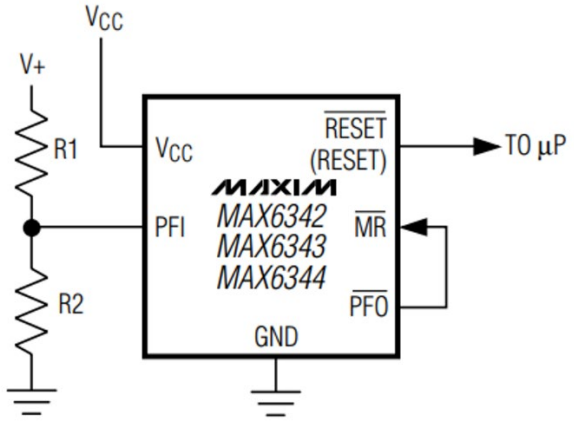
The $t_{warning}$ permits implementing a method for monitoring the input power supply (12V or 5V) and providing advanced warning about the power collapse. When detected early, the SoC specific power supplies (VDD_NT, VDD_EXT, and so forth) are within operational range and permit the power failure detection circuit to act. The detection circuit notifies the SoC to start the safe state and power down in a predictable way. So once the time SoC specific power rails decrease below operation specifications, the SoC has transitioned into the safe state.

Many power monitoring ICs exist that can monitor the power supply. However, to minimize the overall bill of materials (BOM) cost, many of the reset-supervisory ICs that control the SoC also come with a feature to monitor the power supply. One such device is the MAX6342 from Analog Devices that provides both reset and power failure detection functionality. This application note uses this device as an example implementation, but the concept remains the same for other power failure monitoring devices.

Power Failure Detection Example

The power-fail comparator in the MAX6342 is independent of the reset output. This IC provides the PFI and PFO pins for power monitoring and uses an internal reference voltage of +1.25V. To build an early-warning circuit for power failure, the input voltage V (for example, 12V or 5V) can be connected to the PFI pin using a voltage divider as shown in Figure 2.

Figure 2: Voltage Divider Used to Detect Power Failure



The engineer should choose the voltage-divider ratio such that the voltage at PFI pin falls below +1.25V just before the input voltage (12V or 5V) decreases below the detection threshold. We can call this threshold value the *power failure threshold*. The voltage assigned as the point when the input power supply drops out. Define the power failure threshold by considering the system sensitivity and the reliability requirements:

- Choosing a threshold with too small a variance from the input power supply nominal voltage (for example, 4.7V as threshold when using a 5V input supply), means high reliability because the circuit can detect the minor voltage drop (0.3V) in source voltage and trigger the power failure circuit. However, this sensitive circuit can result in intermittent false triggers due to power supply fluctuations.
- Similarly, choosing a significantly lower threshold (for example, 2.5V) can guard against power line fluctuations, but greatly delays the power failure detection as to be almost useless. Waiting for the source voltage to decrease below such a threshold means that there is a good chance that some of the SoC power supplies (VDD_INT, VDD_EXT, so forth) would have also started to decrease. Choosing the right threshold <emphasis> that is immune to power line fluctuations and detects power failure early enough is critical.

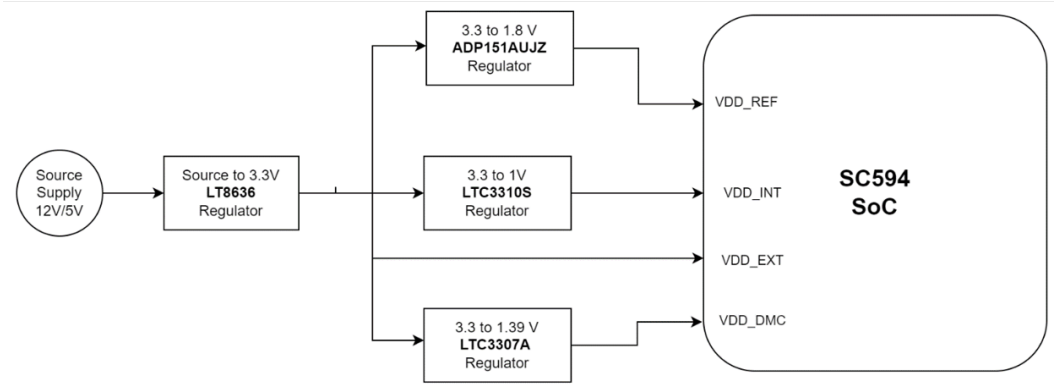
When the input voltage falls below this threshold voltage, the voltage divider circuit chosen ensures that the input to PFI has decreased below 1.25V. This triggers the PFO pin to drive low. This can be used to interrupt the SoC for an orderly shutdown or any other action.

Timing Analysis

The time between the power failure detection and the time that the SoC power supplies remain in operational range ($t_{warning}$) is critical for determining the efficacy of the power failure detection. In this section the results of the experiments and circuit simulations done to estimate and analyze the time available to take the safe state action before the SoC power rails voltage decreases, are presented.

The analysis was done on the ADSP-SC594 SOM evaluation platform. Figure 3 shows a block diagram of the power delivery circuit designed for this evaluation board.

Figure 3: Power Delivery Circuit Example for the ADSP-SC594 Chip



The LT8636 regulator generates 3.3V from the input voltage source which is 12V or 5V. The 3.3V sources the VDD_EXT power domain for the ADSP-SC594. The regulator also feeds:

- An LTC3310S to derive 1.0V for VDD_INT
- An LTC3307A to derive 1.39V for VDD_DMC
- An ADP151AUJZ to derive 1.8V for VDD_REF

Board Simulation Results

Board power-down simulations were done using the LTspice simulator. The simulations performed help understand the power down timing of different power rails when the source power supply is abruptly turned off. This was simulated for different loading current conditions for each power supply, especially the VDD_INT which has the highest power consumption of any power rail.

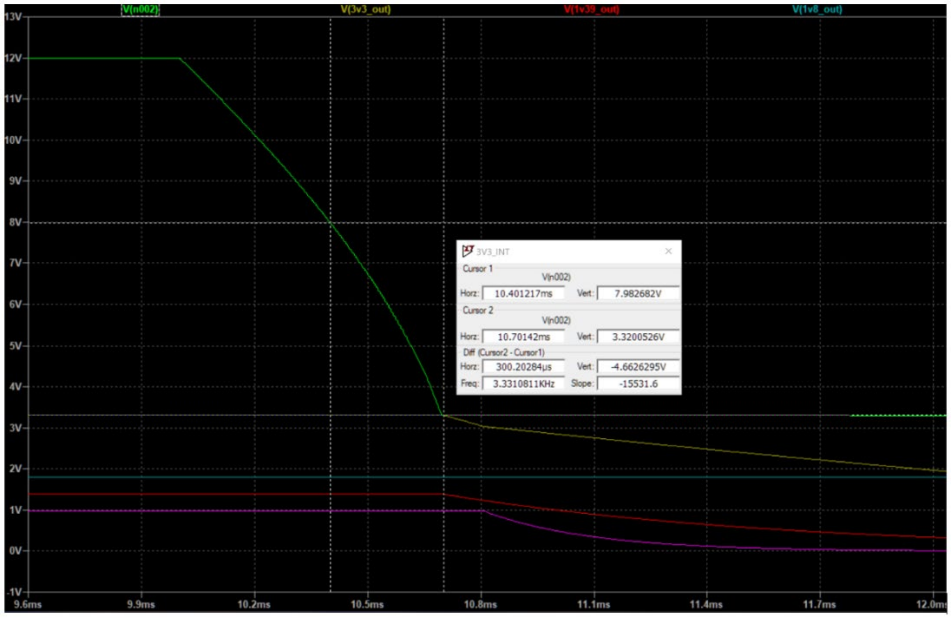
Table 1: Power-down Simulation Case Parameters

Case Number and Name	Source Voltage	Threshold Voltage	Current Draw on SoC Power Rails VDD_INT, VDD_EXT, VDD_DMC, VDD_REF
1. Low Current Consumption	12V	8V	VDD_INT = 1A VDD_EXT = 100 mA VDD_DMC = 100 mA VDD_REF = 100 mA
2. Maximum Current Consumption	12V	8V	VDD_INT = 6A VDD_EXT = 1A VDD_DMC =600 mA VDD_REF = 100 mA
3. Large Threshold Voltage Difference	5V	4V	VDD_INT = 800 mA VDD_EXT = 50 mA VDD_DMC =30 mA VDD_REF = 10 mA
4. Small Threshold Voltage Difference	5V	4.5V	VDD_INT = 1A VDD_EXT = 100 mA VDD_DMC =100 mA VDD_REF = 100 mA

Case Number and Name	Source Voltage	Threshold Voltage	Current Draw on SoC Power Rails VDD_INT, VDD_EXT, VDD_DMC, VDD_REF
5. Maximum Power Consumption	5V	4.5V	VDD_INT = 6A VDD_EXT = 1A VDD_DMC =600 mA VDD_REF = 100 mA

Case 1 - Low Current Consumption (12V)

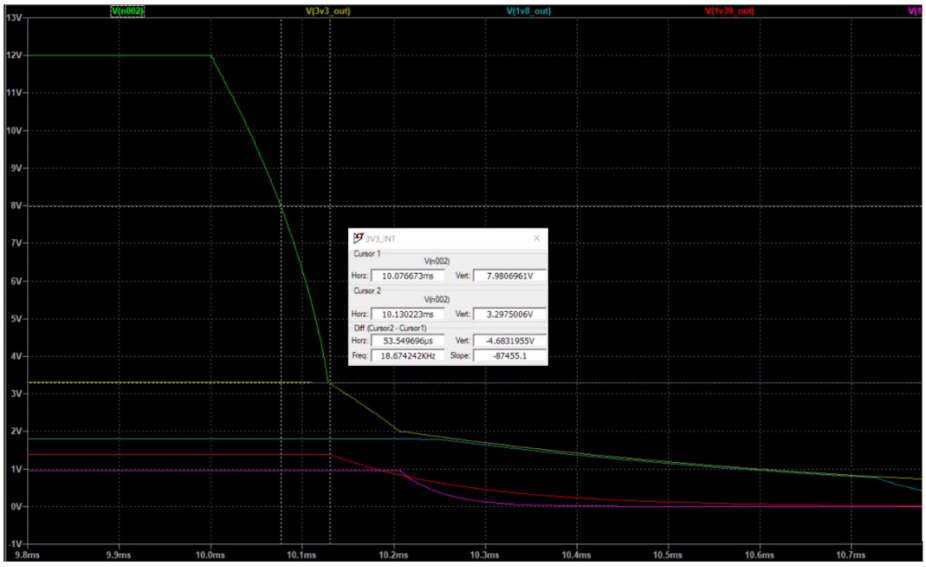
Figure 4: Warning Time Measured for Low Current Consumption (12V) is 300.2 µs



Because the current consumption on different processor power rails is low for this case, the time it takes for one of the power rails to decrease is longer. The time from the 12V crossing the threshold of 8V and VDD_EXT (the earliest to start decreasing) starting to decrease is 300.2 µs.

Case 2 - High Current Consumption (12V)

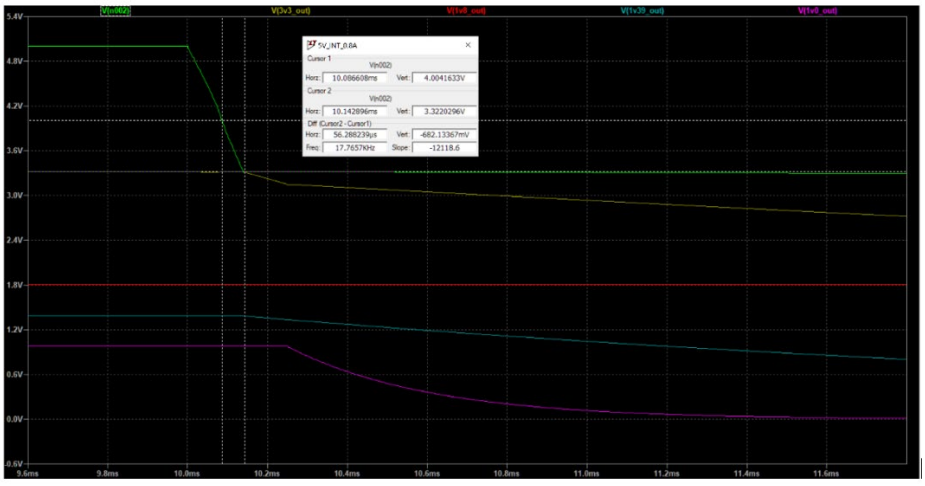
Figure 5: Warning Time Measured for Maximum Current Consumption (12V) is 53.5 µs



This case simulates the maximum current consumption on all the power rails (which may never happen in practice) and represents the worst case in terms of a power down scenario. Because the current consumption is high, the time it takes for one of the power rails to decrease is comparatively less. The warning time from the 12V crossing the threshold of 8V and VDD_EXT (the earliest to start decreasing) starting to decrease is 53.5 µs.

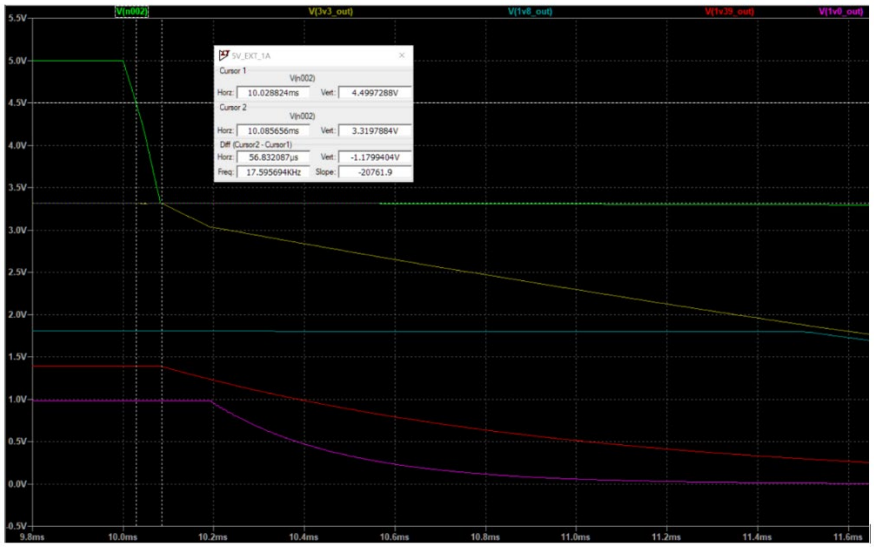
Case 3 - Large Threshold Voltage Difference

Figure 6: Warning Time Measured for Large Threshold Voltage (5V) is 56.2 µs



Case 4 - Small Threshold Voltage Difference

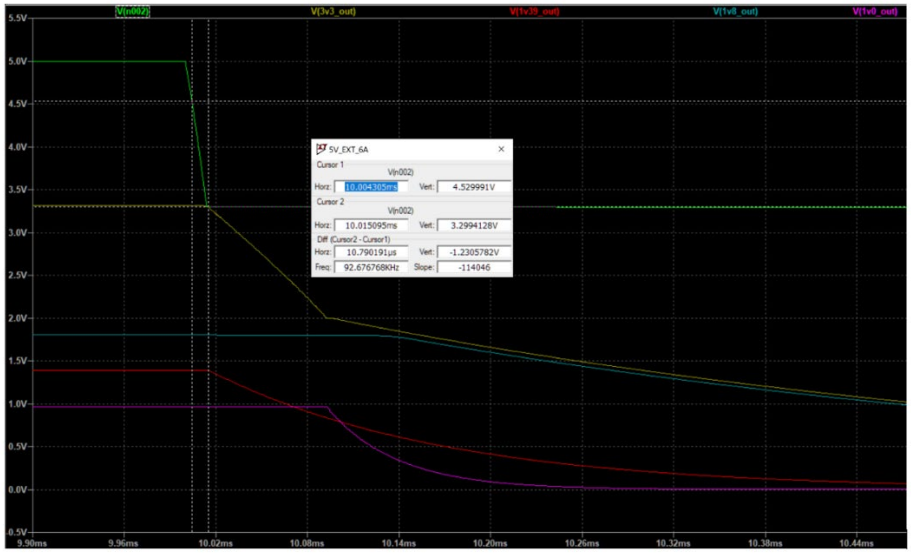
Figure 7: Warning Time Measured for Small Threshold Voltage (5V) is 56.8 µs



Because the source voltage is 5V, as compared to a 12V supply, there is less time available before the SoC power domains start to collapse. The time from the 5V crossing the threshold of 4.5V and VDD_EXT (the earliest to start decreasing) starting to decrease is 56.8 µs.

Case 5 - Maximum Power Consumption

Figure 8: Warning Time Measured for Maximum Power Consumption (5V) is 10.8 us



This represents the worst case with maximum power consumption in all power rails and the source voltage of 5V, thus the warning time when the SoC power domains start to collapse is the minimum. The time from the 5V crossing the threshold of 4.5V and VDD_EXT (the earliest to start decreasing) starting to decrease is 10.8 µs.

Board Simulation Results Summary

The five cases were performed to understand the warning time calculated for different power supplies, different thresholds, and varied power consumption. In Table 2, the Warning Time is the time difference between the Source Voltage decreasing below the Threshold Voltage and the earliest time that the SoC power rails begin collapsing. Collapse is usually indicated by decreasing VDD_EXT voltage.

Table 2: Power-down Simulation Results

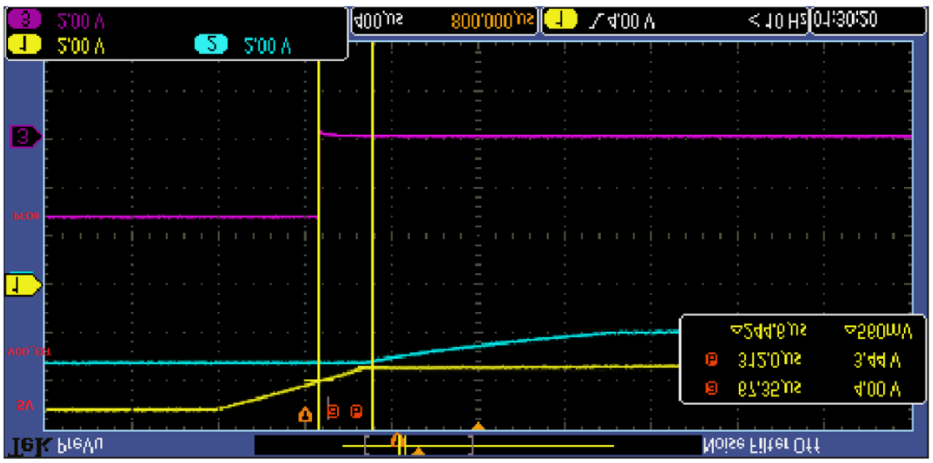
Case Number and Name	Source Voltage	Threshold Voltage	Warning Time ($T_{warning}$) Time between Source Threshold Voltage and Earliest SoC Power Rails Start Decreasing
1. Low Current Consumption	12V	8V	300.2 µs
2. Maximum Current Consumption	12V	8V	53.5 µs
3. Large Threshold Voltage Difference	5V	4V	56.2 µs
4. Small Threshold Voltage Difference	5V	4.5V	56.8 µs
5. Maximum Power Consumption	5V	4.5V	10.8 µs

Board Testing

To correlate the simulation results, Analog Devices did an experiment for power down on the EV-SC594-SOM board, a source voltage of 5V and threshold voltage of 4.0V. The current consumption was VDD_INT load current of approximately 800 mA, with other power domains have very small loading (few 10's of milliamperes).

On the board the time delay seen is approximately 244 µs which is much better than 56.2 µs seen in the simulation for 5V supply case (Case #3 in the Board Simulation Results Summary section). The board results are better because the simulation does not model the stray capacitance on the board that reduces the voltage decrease rate and increases the warning time.

Figure 9: EV-SC594-SOM Board Test with Small Current Consumption (5V)



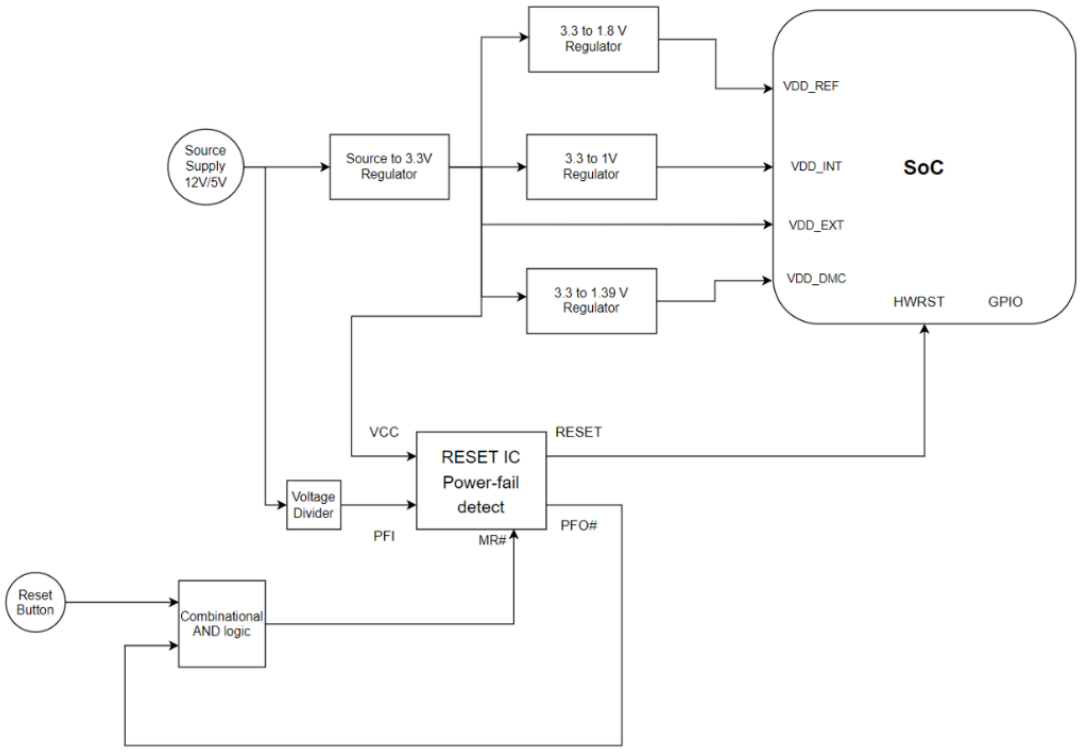
Implementing Power Failure Detection

The following sections describe implementations that demonstrate how power failure detection can be implemented using the ADSP-SC594/ADSP-21593 processors (also applicable to other processors in the Applicable Processors section on page 1). The detection provides advance warning to the processor during the power down and subsequently starts a safe processor state transition.

Transition to Reset on Power Failure

For this technique, the source power supply is monitored using the power failure detection circuit (MAX6342). In steady state when source voltage is stable, the PFO# pin voltage output is high (3.3V). When the source voltage starts to decrease, SoC power supplies are still at nominal voltages because the input to all the downstream regulators remains above the required input voltage of these regulators. When source voltage decreases below the set threshold voltage (voltage divider causing the PFI voltage to decrease below 1.25V), the PFO# pin asserts low.

Figure 10: Block Diagram for Transition to Reset on Power Failure



The PFO# is fed back to the MR# pin of the MAX6342 though an AND gate that has the reset input from the board (push-button). This causes the MR to be asserted low which drives the RESET pin of the MAX6342 low; because this is connected to the SoC reset input pin (SYS_HWRST). This immediately puts the SoC in the reset.

The latency for this RESET assertion equals the time when the source voltage decreases below set threshold is the result of three delays or **Delay** = PFI to PFO Delay + MR to Reset Delay + AND gate propagation delay:

- PFI to PFO Delay =3 µs (MAX62432 datasheet) typical value
- MR to Reset Delay = 0.1 µs typical value
- AND gate propagation delay is usually less than 0.05 µs for most of the devices

Delay = less than 4 µs or of a similar order, depending on the power failure detection device

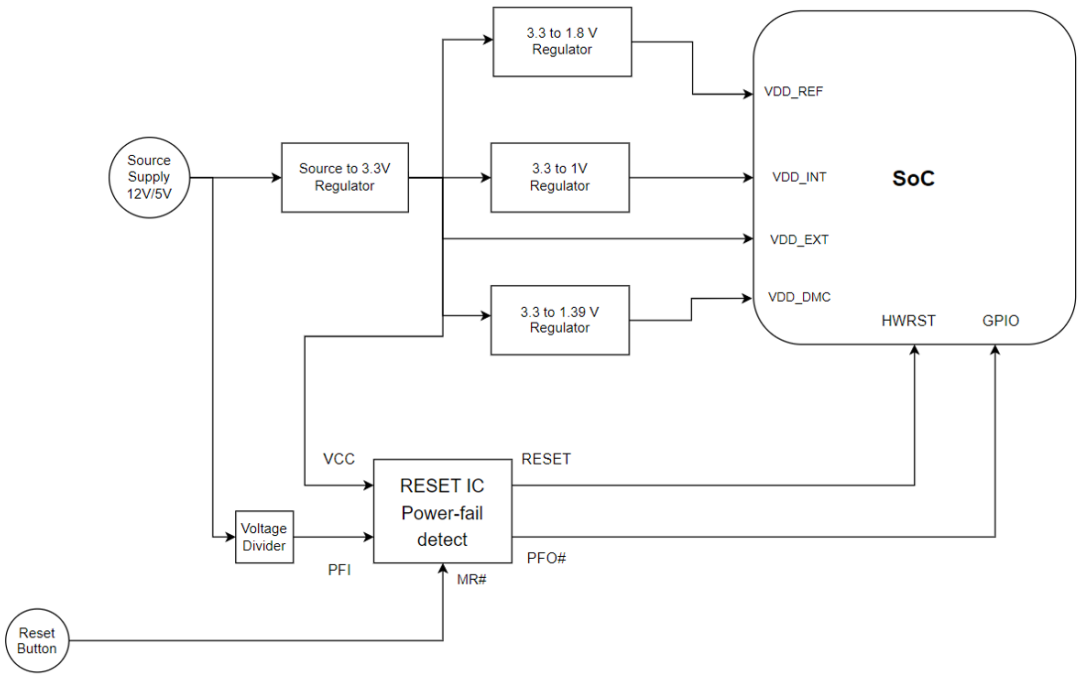
As displayed in the power down simulations, the warning time (when the SoC power supplies remain at their nominal voltage after the source voltage decreases below the threshold, 8V for 12V source and 4.5V for 5V source) exceeds 10.8 µs, even for the worst-case SoC power consumption. There is very high probability that this power detection scheme can put the SoC in reset before the SoC power rails start decreasing, ensuring all the SoC operations are stopped and that all the external pins are in known reset state.

Another variation of this technique is to connect PFO# output directly to the SYS_HWRST input of the SoC, rather than through the reset IC. In this case the PFO# can be ANDed with the RESET output of the reset IC and fed to the SYS_HWRST.

Transition to Safe State on Power Failure

In this technique, the source power supply is monitored using the power failure detection circuit (MAX6342). As explained earlier, for the case where a power failure when source voltage drops below the set threshold, the PFO# pin asserts low. For this approach, the PFO# output is connected to one of the GPIO pins of the SoC.

Figure 11: Transition to Safe State on Power Failure Block Diagram



Software can configure this GPIO to detect a falling edge transition on this pin. For a power failure, the falling edge of the PFO# triggers the GPIO, signaling the SoC about the power loss. With this warning the SoC can take require safe state measures before the actual power down. For the family of processors described in Applicable Processors on page 1 (and specifically ADSP-SC594/ADSP-21593), the GPIO can be configured to generate the trigger that is used to trigger another block (like MDMA) to write critical registers in the processor and bring the block of the processor to known state. Because the trigger mechanism is a low-latency process it can trigger the action in fixed time. But it is limited in its capability to be configured to a safe state before powering down.

A more flexible approach enables the GPIO to generate the interrupt (configured for highest priority possible). Once this interrupt fires (due to power failure), interrupt handling software can more flexibly implement the key actions necessary for a safe state.

As noted earlier, for worst case power draw, the power failure circuit offers the advance waning time providing a minimum of 11 µs for processor to act. At a 1 GHz core clock frequency, this translates to approximately 11,000 core clock cycles to execute the safe state code before the power rails of SoC decreases. This is ample time to implement a critical safe state operation.

In an example test, the following code block for the GPIO interrupt handler can put the OSPI controller in disabled state to avoid the problem described in OSPI During Power Down section on page 2.

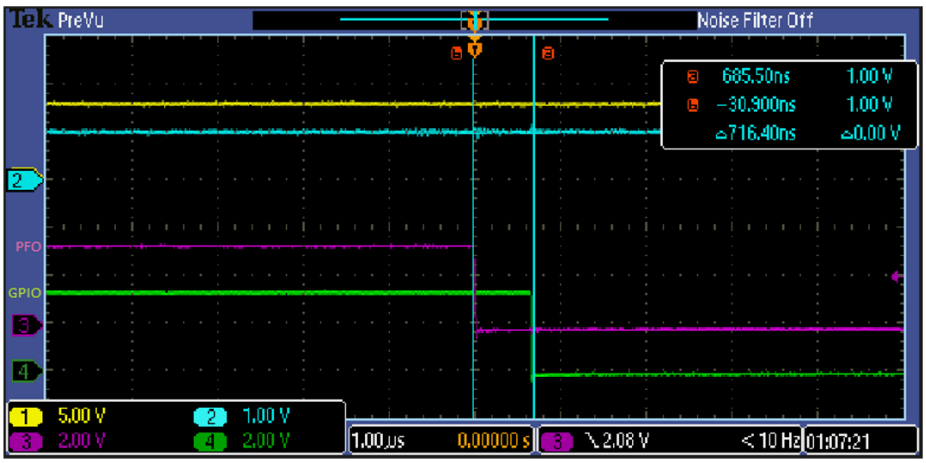
```
    if(ePinInt == PIN_INTERRUPT1)
{
    count++;

    // Disable OSPI peripheral and OSPI pin mux
    *pREG_OSPI0_CTL = 0;
    *pREG_PORTA_FER = 0;

    adi_gpio_Toggle(GPIO_OUTPUT_PORT, GPIO_OUTPUT_PIN);
}
```

The latency from PFO# assertion to the GPIO output pin toggled after the OSPI is disabled is just .717 µs.

Figure 12: Warning Time Measured Between PF0# Assertion GPIO Output Pin Toggled



The overall time taken from the power failure to the OSPI controller getting disabled is sum of PFI to PFO Delay, ISR latency, and execution. That adds up to less than 3.8 µs (PFI to PFO Delay typical value is 3 µs), which is less than the 11 µs warning time available in the worst case processor power load shown in Table 2: Power-down Simulation Results on page 10.

References

[1] *ADSP-SC582/SC583/SC584/SC587/SC589/ADSP-21583/21584/21587 Data Sheet* Rev C. June 2023. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/data-sheets/ADSP-SC582_583_584_587_589_ADSP-21583_584_587.pdf

[2] *ADSP-SC570/SC571/SC572/SC573/ADSP-21571/21573 Data Sheet* Rev B. June 2018. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/data-sheets/ADSP-SC570-571-572-573-ADSP-21571-573.pdf

[3] *ADSP-21562/21563/21565/21566/21567/21569 Data Sheet* Rev D. June 2023. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/data-sheets/adsp-21562-21563-21565-21566-21567-21569.pdf

[4] *ADSP-21591/21593/21594/ADSP-SC591/SC592/SC594 Data Sheet* Rev A, April 2022. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/data-sheets/adsp-21591-593-594-adsp-sc591-sc592-sc594.pdf

[5] *ADSP-SC595/SC596/SC598 Data Sheet* Rev PrE, July 2022. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/data-sheets/adsp-sc595-sc596-sc598.pdf

[6] *ADSP-2159x/ADSP-SC591/592/594 SHARC+ Processor Hardware Reference.* Rev PrE, July 2022. Analog Devices, Inc. https://www.analog.com/media/en/dsp-documentation/processor-manuals/adsp-2159x-sc591-592-594-hrm.pdf

[7] *Maxim MAX6342–MAX6345 6-Pin µP Reset Circuit with Power-Fail Comparator.* Rev 2; 12/05. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/data-sheets/MAX6342-MAX6345.pdf

[8] *EV-SC594-SOM ADSP-SC594 System On Module.* Rev B, September 2020. Analog Devices, Inc. https://www.analog.com/media/en/technical-documentation/eval-board-schematic/ev-sc594-som-schematic.pdf

[9] *EV-SC594-SOM® Manual, Rev 1.0, April 2021. Analog Devices, Inc.* https://www.analog.com/media/en/technical-documentation/user-guides/ev-sc594-som_manual.pdf

Document History

Revision	Description
Rev 1 – September 5, 2023 *by Nabeel Shah* *and Shivakumar Puran*	Initial Release