Functional Safety Information

Functional Safety Manual for DLP4620S-Q1, DLPC231S-Q1, and TPS99000S-Q1

Table of Contents

List of Figures

List of Tables

1 Introduction

This document is a functional safety manual for the Texas Instruments DLP4620S-Q1 chipset. The specific orderable part numbers supported by this functional safety manual are as follows:

- DLP4620S-Q1 (Orderable Part #: DLP4620SAFQXQ1)
- DLPC231S-Q1 (Orderable Part #: DLPC231STZDQQ1)
- TPS99000S-Q1 (Orderable Part #: TPS990STPZPQ1, TPS990STPZPRQ1)

This functional safety manual provides information needed by system developers to help in the creation of a functional safety system using the DLP4620S-Q1 chipset. This document includes:

- An overview of the chipset architecture
- An overview of the development process used to decrease the probability of systematic failures
- An overview of the functional safety architecture for management of random failures
- The details of architecture partitions and implemented functional safety mechanisms

The following information is documented in the *DLP4620S-Q1 Functional Safety Analysis Report* and is not repeated in this document:

- Summary of failure rates (FIT) of the component.
- Summary of functional safety metrics of the hardware components for targeted standards (for example IEC 61508, ISO 26262, and so forth).
- Quantitative functional safety analysis (also known as FMEDA, Failure Modes, Effects, and Diagnostics Analysis) with detail of the different parts of the chipset, allowing for customized application of functional safety mechanisms. For the DLP4620S-Q1 chipset, TI will provide a total of three FMEDAs, one for each component of the chipset.
- Assumptions used in the calculation of functional safety metrics.

The user of this document should have a general familiarity with the DLP4620S-Q1 chipset. For more information, refer to the *DLP4620S-Q1* data sheet. This document is intended to be used in conjunction with the pertinent data sheets, technical reference manuals, and other chipset documentation.

For information that is beyond the scope of the listed deliverables, contact your TI sales representative or go to http://www.ti.com/technologies/functional-safety/overview.html.

Trademarks

TI E2E™ is a trademark of Texas Instruments.
All trademarks are the property of their respective owners.

2 DLP4620S-Q1 Chipset Functional Safety Capability

This section summarizes the component functional safety capability.

The DLP4620S-Q1 chipset:

- Was not developed according to the requirements of any functional safety standard.
- FIT rates and failure mode distributions are provided as part of the *DLP4620S-Q1 Functional Safety Analysis Report* for customers to calculate random fault integrity metrics.
- Recommendations are provided in this Functional Safety Manual for external safety mechanisms that may provide coverage for component failure modes.
- TI recommends that this component is integrated into the system through the strategy of "evaluation of hardware element" (ISO 26262-8:2018 clause 13)

3 Development Process for Management of Systematic Faults

For functional safety development, it is necessary to manage both systematic and random faults. Texas Instruments follows a new-product development process for all of its components which helps to decrease the probability of systematic failures. This new-product development process is described in Section 3.1. Components being designed for functional safety applications will additionally follow the requirements of TI's functional safety development process, which is described in Section 3.2.

3.1 TI New-Product Development Process

Texas Instruments has been developing components for automotive and industrial markets since 1996. Automotive markets have strong requirements regarding quality management and product reliability. The TI new-product development process features many elements necessary to manage systematic faults. Additionally, the documentation and reports for these components can be used to assist with compliance to a wide range of standards for customer's end applications including automotive and industrial systems (e.g., ISO 26262-4, IEC 61508-2).

This component was developed using TI's new product development process which has been certified as compliant to ISO 9001 / IATF 16949 as assessed by Bureau Veritas (BV).

The standard development process breaks development into phases:

- Assess
- Plan
- Create
- Validate

Figure 3-1 shows the standard process.

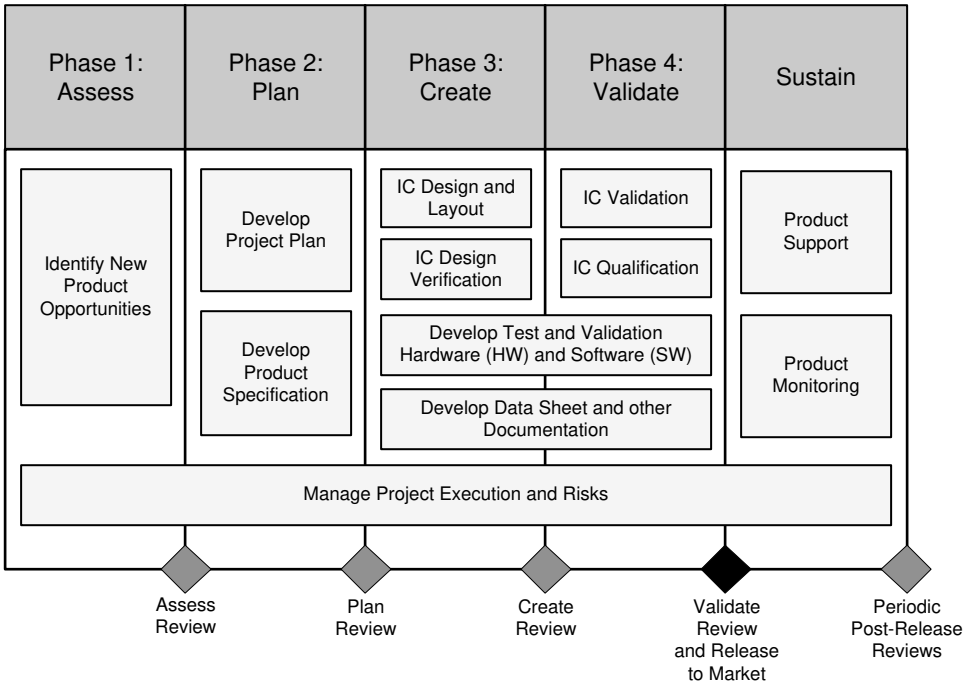

Figure 3-1. TI New-Product Development Process

3.2 TI Functional Safety Development Process

The TI functional safety development flow derives from ISO 26262 and IEC 61508 a set of requirements and methodologies to be applied to semiconductor development. This flow is combined with TI's standard new product development process to develop TI functional safety components. The details of this functional safety development flow are described in the TI internal specification - Functional Safety Hardware.

Key elements of the TI functional safety-development flow are as follows:

- Assumptions on system level design, functional safety concept, and requirements based on TI's experience with components in functional safety applications
- Qualitative and quantitative functional safety analysis techniques including analysis of silicon failure modes and application of functional safety mechanisms
- Base FIT rate estimation based on multiple industry standards and TI manufacturing data
- Documentation of functional safety work products during the component development
- Integration of lessons learned through multiple functional safety component developments, functional safety standard working groups, and the expertise of TI customers

Table 3-1 lists these functional safety development activities which are overlaid atop the standard development flow in Figure 3-1.

Refer to Appendix B for more information about which functional safety lifecycle activities TI performs.

The customer facing work products derived from this TI functional safety process are applicable to many other functional safety standards beyond ISO 26262 and IEC 61508.

Table 3-1. Functional Safety Activities Overlaid on top of TI's Standard Development Process

Assess	Plan	Create	Validate	Sustain and End-of-Life
Determine if functional safety process execution is required	Define component target SIL/ASIL capability	Develop component level functional safety requirements	Validate functional safety design in silicon	Document any reported issues (as needed)
Nominate a functional safety manager	Generate functional safety plan	Include functional safety requirements in design specification	Characterize the functional safety design	Perform incident reporting of sustaining operations (as needed)
End of Phase Audit	Verify the functional safety plan	Verify the design specification	Qualify the functional safety design (per AEC-Q100)	Update work products (as needed)
	Initiate functional safety case	Start functional safety design	Finalize functional safety case	
	Analyze target applications to generate system level functional safety assumptions	Perform qualitative analysis of design (i.e. failure mode analysis)	Perform assessment of project	
	End of Phase Audit	Verify the qualitative analysis	Release functional safety manual	
		Verify the functional safety design	Release functional safety analysis report	
		Perform quantitative analysis of design (i.e. FMEDA)	Release functional safety report	
		Verify the quantitative analysis	End of Phase Audit	
		Iterate functional safety design as necessary		
		End of Phase Audit		

4 DLP4620S-Q1 Chipset Overview

The DLP4620S-Q1 chipset consisting of the DLP automotive Digital Micromirror Device (DMD), DLPC231S-Q1 DMD controller, and TPS99000S-Q1 system management and illumination controller, provides the capability to achieve a high performance augmented reality Head-Up Display or a windshield cluster display. Figure 4-1 shows a block diagram for a Head-Up Display or Windshield Cluster using the DLP4620S-Q1 chipset.

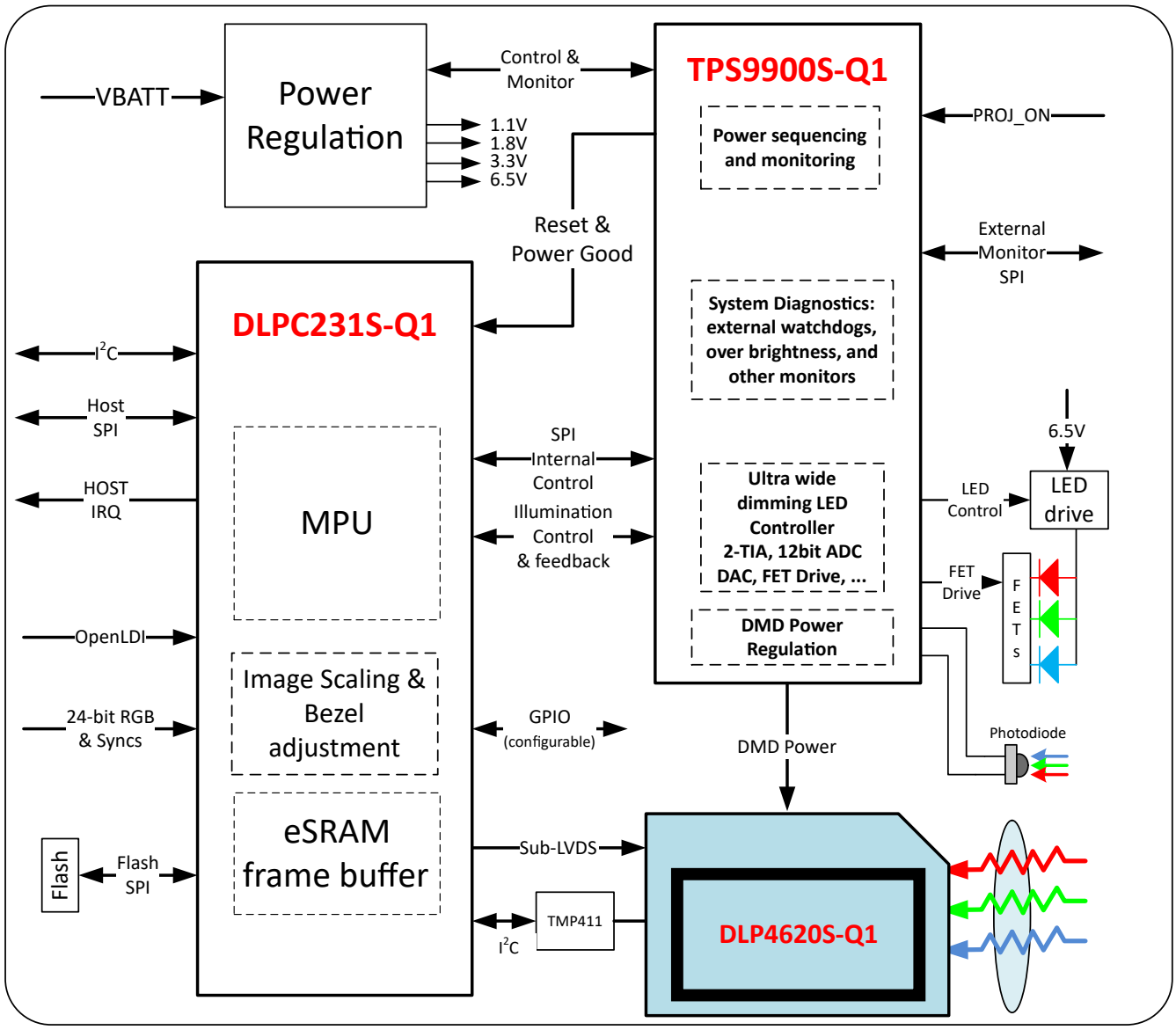

Figure 4-1. DLP4620S-Q1 Chipset Block Diagram

4.1 Targeted Applications

The DLP4620S-Q1 chipset is targeted at general-purpose functional safety applications. This is called Safety Element out of Context (SEooC) development according to ISO 26262-10. In this case, the development is done based on assumptions on the conditions of the semiconductor component usage, and then the assumptions are verified at the system level. This method is also used to meet the related requirements of IEC 61508 at the semiconductor level. This section describes some of the target applications for this component, the component safety concept, and then describes the assumptions about the systems (also know as Assumptions of Use or AoU) that were made in performing the safety analysis.

Example target applications include, but are not limited to, the following:

- Automotive Head-Up Display
- Automotive windshield cluster

4.2 DLP4620S-Q1 Chipset Functional Safety Concept

Typical applications for the DLP4620S-Q1 chipset include an Augmented Reality (AR) HUD and Windshield Cluster. This section discusses some typical hazards in these applications and how this chipset can help minimize the risk of these hazards.

For risk minimization, this chipset includes many Built-In Self Tests (BISTs). These are monitoring and diagnostic functions that are implemented in the chipset to detect and act upon failure conditions. A general overview of BISTs with regards to typical hazards is provided below. For full implementation details, please refer to the *DLPC231S-Q1 Programmer's Guide for Display Applications*.

4.2.1 Typical Hazards

Well-known hazards in a HUD and Windhsield Cluster include:

- Corruption of image content such that it prevents the driver from seeing obstacles or traffic on the road ahead
- Excessively bright LEDs that results in a very bright image that glares the driver

Note: The list of hazards above may not be exhaustive. The OEM and system integrator should consider any other risks involved.

4.2.2 Chipset Architecture

The architecture of the DLP chipset helps minimize risk of hazards through independent monitoring and distributed responsibility. For example, the TPS independently monitors the DLPC using watchdogs. Many Built-In Self Tests (BISTs) of the chipset also distribute the responsibility amongst the devices. For example, the TPS is responsible for taking ADC measurements, however, the DLPC has the software to analyze the measurements and detect error conditions.

The architecture of this chipset makes it more robust against random faults.

4.2.3 Built-In Self Tests

The DLP4620S-Q1 chipset includes a wide variety of Built-In Self Tests (BISTs). These BISTs, are the mechanisms used to monitor and diagnose the chipset, and protect against the hazards described in Section 4.2.1. Figure 4-2 and Figure 4-3 give a brief overview of the BISTs in the DLP4620S-Q1 chipset for protecting against functional safety related faults. These BISTs are described in more detail in Section 6.3.

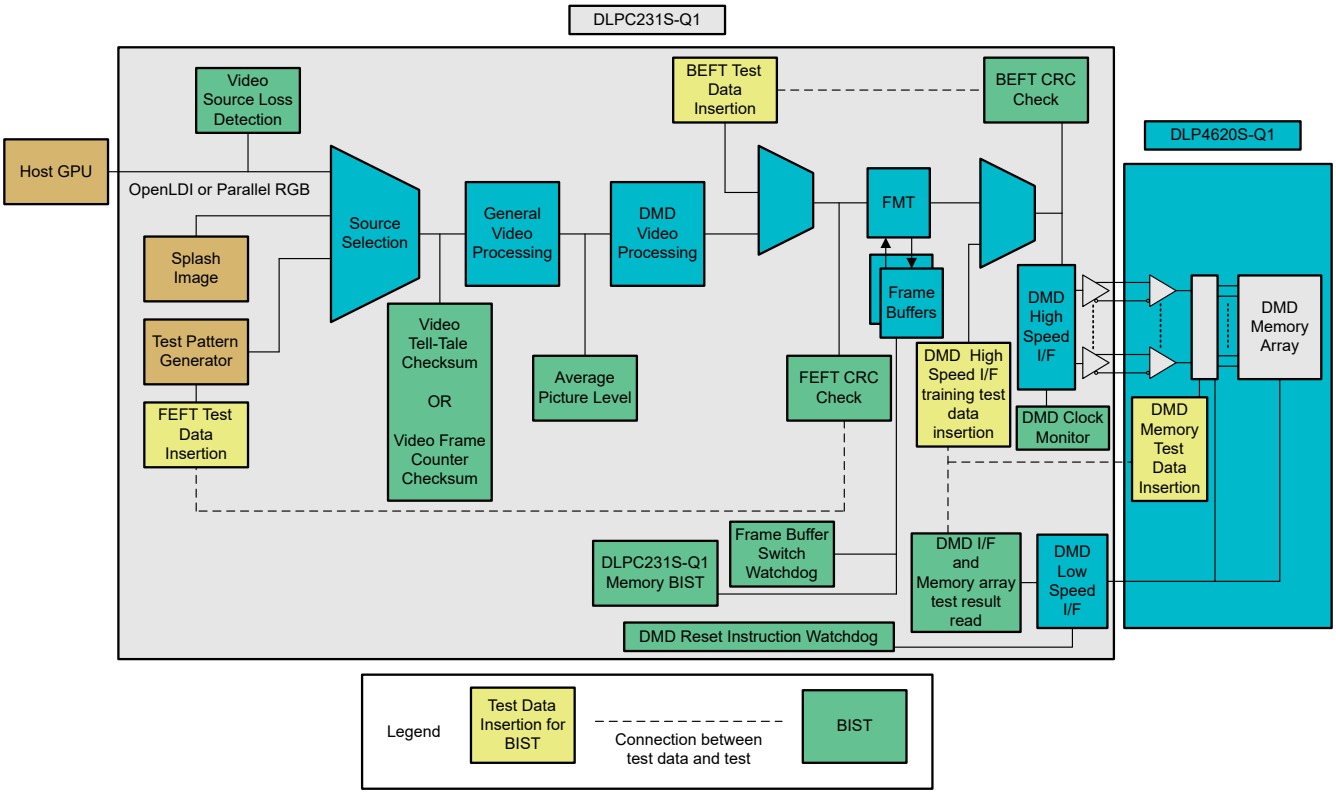

Figure 4-2. DLP4620S-Q1 Video Path With Diagnostics

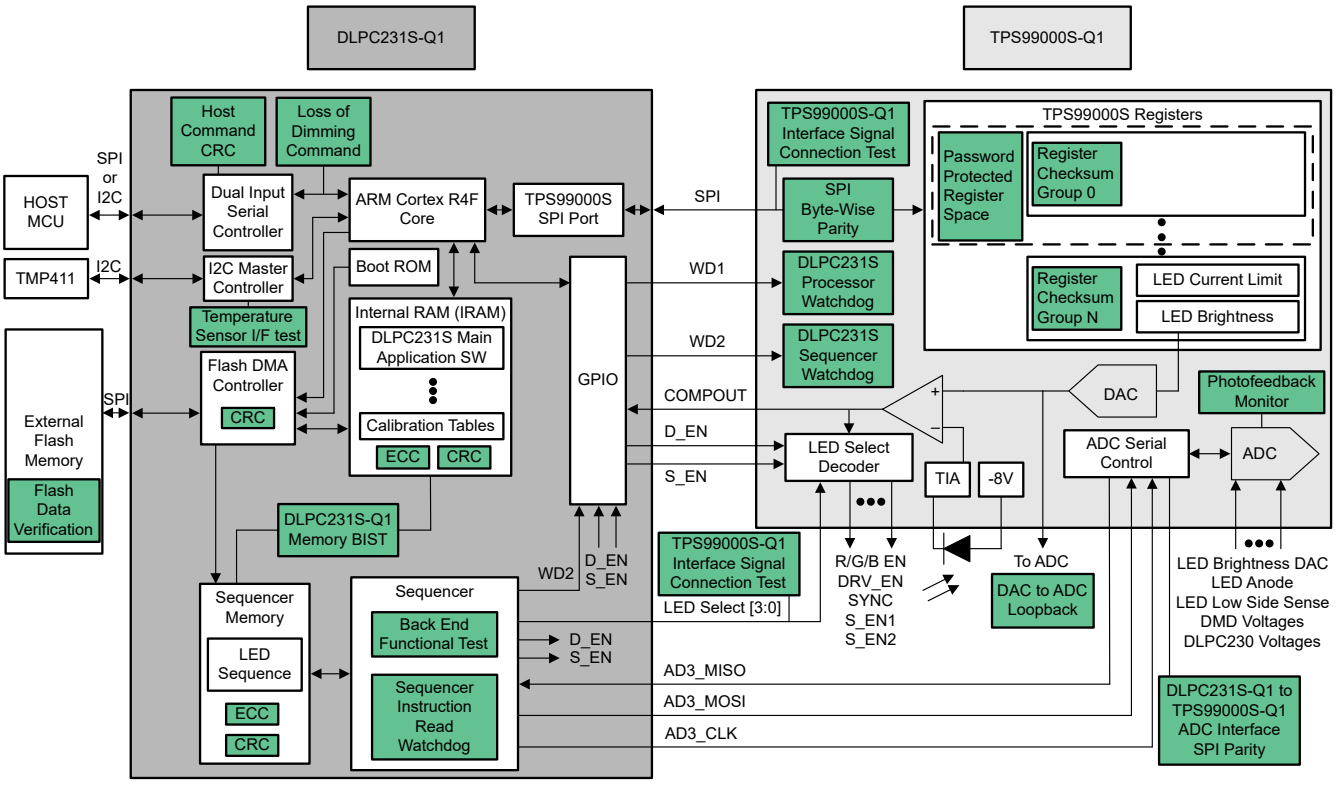

Figure 4-3. Illumination Control Architecture With Diagnostics

4.3 Functional Safety Constraints and Assumptions

In creating a functional Safety Element out of Context (SEooC) concept and doing the functional safety analysis, TI generates a series of assumptions on system level design, functional Safety Element out of Context (SEooC), and requirements. These assumptions (sometimes called Assumptions of Use) are listed below. Additional assumptions about the detailed implementation of safety mechanisms are separately located in Section 6.3.

The DLP4620S-Q1 Functional Safety Analysis was done under the following system assumptions:

- **[SA_1]** The system integrator shall follow all requirements in the component data sheet.
- **[SA_2]** The system integrator shall enable all BISTs.

During integration activities these assumptions of use and integration guidelines described for this chipset shall be considered. Use caution if one of the above functional safety assumptions on this chipset cannot be met, as some identified gaps may be unresolvable at the system level.

5 Description of Hardware Component Parts

A semiconductor component can be divided into parts to enable a more granular functional safety analysis. This can be useful to help assign specific functional safety mechanisms to portions of the design where they provide coverage ending up with a more complete and customizable functional safety analysis. This section includes a brief description of the various blocks of the three chipset components. The quantitative functional safety analysis is done according to these partitions. Partitions for each device are given in the tables below.

Table 5-1. DLPC231S-Q1 Blocks

Block Name	Block Function
VGP	Video and Graphics Processor. Receives input video data and generates splash images or test patterns. Performs video processing functions such as scaling and color space conversion.
RTP	Real-Time Processor. ARM micro-processor core and related memories.
RSC	Real-Time System Control. Timing control for LEDs, DMD mirror transitions, and ADC measurements. Includes hardware processing blocks and associated memories.
FMT	Formatter and Universal Memory Controller. Converts data output from the VGP into single color images that are displayed on the DMD. Includes the SRAM frame buffers. Data is received from the VGP, processed, and stored into the frame buffer. Data is output from the frame buffer to the DMD based on instructions from the RSC.
SSF	Clock generation for various clock domains in the DLPC231S-Q1.
DDI	DMD data interface. High speed interface for outputting data from DLPC231S-Q1 to DMD.
FPD	OpenLDI input video port.
RTP BROM	Boot ROM that initiates loading of software from external flash to internal RAM and performs boot tests.

Table 5-2. TPS99000S-Q1 Blocks

Block Name	Block Function
AAC	ADC control including the TPS99000S-Q1 to DLPC231S-Q1 AD3 interface.
CSR	Configuration status registers.
DEG	Deglitching for signals.
DTV	Data transfer validation. DLPC231S-Q1 to TPS99000S-Q1 SPI port and related functions.
ILM	Illumination control.
PSC	Power state controller.
SSF	Secondary SPI port for diagnostics.
ROM	ROM used for storing device trim data.

Table 5-3. DLP4620S-Q1 Blocks

Block Name	Block Function
SRAM	SRAM cells under micro-mirror layer. Data loaded into SRAM determines state of each mirror.
IO	High speed interface that receives the video data from the DLPC231S-Q1.
SCTRL	Instruction decoder for data received over IO.
Reset Ctrl	Mirror transition control.
LSIF	Low speed interface for DMD configuration and mirror reset voltage control.

5.1 Description of System Level Built In Self Test (BISTs)

In order to integrate and evaluate this chipset into an ISO26262 certified system, TI recommends validating BIST functionality in-system. Recommended methods for testing each BIST are listed in Table 5-4. For cases that require batch command sets or special software builds to induce failures, please contact TI.

Table 5-4. Recommended Methods for Testing BISTs

BIST	Method to Induce Failure	Related HOST SPI Command
DLPC231S-Q1 Host Command CRC	Send SPI command to DLPC231S-Q1 with incorrect CRC	51h
Video Source Loss Detection	Remove video source	N/A
Video Tell-Tale Checksum	Use one of the following methods: 1. Modify source without changing expected checksum 2. Change expected checksum 3. Change checksum check region	2Bh / 2Ch
Video Frame Counter Checksum	Use one of the following methods: 1. Modify source to change frame counter 2. Change frame count check region	2Bh / 2Ch
Average Picture Level	1. Set input image to full white 2. Set APL level to 100	2Fh / 30h
Loss of Dimming Command	Enable test then do not send any dimming commands	33h / 34h
Photo Feedback Monitor	Disconnect photo-diode on system	N/A
DLPC231S-Q1 Processor Memory ECC	This failure can only be induced by TI. Please contact TI for more information.	N/A
Flash Table Transport CRC	Software build required to induce failure. Please contact TI	N/A
Frame Buffer Swap Watchdog	Batch command set required to induce failure. Please contact TI	N/A
Sequencer Instruction Read Watchdog	Batch command set required to induce failure. Please contact TI	N/A
DMD Reset Instruction Watchdog	Batch command set required to induce failure. Please contact TI	N/A
DLPC231S-Q1 System Voltage Monitor	Build and program flash with modified VMAIN threshold OR Adjust VMAIN with hardware until error is detected	N/A
DLPC231S-Q1 DMD Voltage Monitor	Software build required to induce failure. Please contact TI	N/A
DMD Clock Monitor	No method for inducing this error. TI performed validation on this test	
DMD High Speed Interface Training	Build and program flash image with incorrect pin mapping. Set system to display mode.	N/A
DMD Low Speed Interface Test	Software build required to induce failure. Please contact TI	N/A
TPS99000S-Q1 DLPC231S-Q1 Processor Watchdog (WD1)	Batch command set required to induce failure. Please contact TI	N/A
TPS99000S-Q1 DLPC231S-Q1 Sequencer Watchdog (WD2)	Batch command set required to induce failure. Please contact TI	N/A
TPS99000S-Q1 Clock Ratio Monitor	Software build required to induce failure. Please contact TI	N/A
TPS99000S-Q1 Register checksum	Batch command set required to induce failure. Please contact TI	N/A
DLPC231S-Q1 Front-End Functional Test	Software build required to induce failure. Please contact TI	N/A
DLPC231S-Q1 Back-End Functional Test	Software build required to induce failure. Please contact TI	N/A
DLPC231S-Q1 Memory BISTs	Software build required to induce failure. Please contact TI	N/A
TPS99000S-Q1 Signal Interface	Disconnect DLPC231S-Q1 to TPS99000S-Q1 SPI or LED Select Interface	N/A
DMD Memory Test	No method for inducing this error. TI performed validation on this test	N/A

Table 5-4. Recommended Methods for Testing BISTs (continued)

BIST	Method to Induce Failure	Related HOST SPI Command
Flash Data Verification	Software build required to induce failure. Please contact TI	N/A
DLPC231S-Q1 Boot ROM CRC	Software build required to induce failure. Please contact TI	N/A
DLPC231S-Q1 Flash Table CRC	Software build required to induce failure. Please contact TI	N/A
DLPC231S-Q1 Main App CRC	Software build required to induce failure. Please contact TI	N/A
DLPC231S-Q1 to TPS99000S-Q1 SPI Byte-Wise Parity	No method for inducing persistent parity error. TI performed software verification on this test	N/A
DLPC231S-Q1 to TPS99000S-Q1 ADC Interface SPI Parity	No method for inducing persistent parity error. TI performed software verification on this test	N/A
TPS99000S-Q1 password protected register space	No method for inducing this error	N/A
DAC to ADC loopback test	Disconnect DLPC231S-Q1 to TPS99000S-Q1 SPI	N/A

6 Management of Random Faults

For a functional safety critical development it is necessary to manage both systematic and random faults. The DLP4620S-Q1 chipset architecture does not include any functional safety mechanisms, which can detect and respond to random faults when used correctly. This section of the document describes the architectural functional safety concept for each sub-block of the DLP4620S-Q1 chipset. The system integrator shall review the recommended functional safety mechanisms in the functional safety analysis report (FMEDA) in addition to this safety manual to determine the appropriate functional safety mechanisms to include in their system. The component data sheet or technical reference manual (if available) are useful tools for finding more specific information about the implementation of these features.

6.1 Fault Reporting

The DLP4620S-Q1 has two major mechanisms for fault reporting: Error History and HOST_IRQ.

6.1.1 HOST_IRQ

For more urgent error conditions, the DLPC231S-Q1 has the HOST_IRQ signal that can be used for interrupt driven programming of the host MCU. The DLPC231S-Q1 asserts this signal high to indicate to the host MCU that a serious system error has occurred. A serious system error is something that TI considers likely to corrupt the display image, and/or create a bright display image, and/or damage one or more chipset devices. This signal can be used to interrupt the host MCU to handle the urgent error.

6.1.2 Error History

The DLPC231S-Q1 stores an error history to indicate which errors have occurred in the system. The error history can be read by the host MCU using SPI or I2C. Full implementation details of the Error History, including error codes are described in the *DLPC231S-Q1 Programmer's Guide For Display Applications*.

6.1.3 Fault Handling

The DLPC231S-Q1 software implements two ways of error handling—error logging and emergency shutdown. All errors detected by the system are logged in the error history. However, for more critical errors, errors that will obviously lead to a bright image, corrupted image, or damaged devices, the DLPC231S-Q1 executes an emergency shutdown.

In emergency shutdown, DLPC231S-Q1 main application software performs the following actions:

- Disables LEDs
- Parks and powers down DMD
- Transitions software to Standby Mode
- Captures errors in error history
- Sets emergency shutdown bit in status
- Asserts HOST_IRQ

Full implementation details of emergency shutdown can be found in the *DLPC231S-Q1 Programmer's Guide For Display Applications*.

6.2 Functional Safety Mechanism Categories

This section includes a description of the different types of functional safety mechanisms that are applied to the design blocks of the DLP4620S-Q1 chipset.

The functional safety mechanism categories are defined as follows:

Component Hardware Functional Safety Mechanisms	A safety mechanism that is implemented by TI in silicon which can communicate error status upon the detection of failures. The safety mechanism may require software to enable its functionality, to take action when a failure is detected, or both.
Component Hardware and Software Functional Safety Mechanisms	A test recommended by TI which requires both, safety mechanism hardware which has been implemented in silicon by TI, and which requires software. The failure modes of the hardware used in this safety mechanisms are analyzed or described as part of

	the functional safety analysis or FMEDA. The system implementer is responsible for analyzing the software aspects for this safety mechanism.
Component Software Functional Safety Mechanisms	A software test recommended by TI. The failure modes of the software used in this safety mechanism are not analyzed or described in the functional safety analysis or FMEDA. For some components, TI may provide example code or supporting code for the software functional safety mechanisms. This code is intended to aid in the development, but the customer shall do integration testing and verification as needed for their system functional safety concept.
System Functional Safety Mechanisms	A safety mechanism implemented externally of this component. For example an external monitoring IC would be considered to be a system functional safety mechanism.
Test for Safety Mechanisms	This test provides coverage for faults on a safety mechanism only. It does not provide coverage for the primary function.
Alternative Safety Mechanisms	An alternative safety mechanism is not capable of detecting a fault of safety mechanism hardware, but instead is capable of recognizing the primary function fault (that another safety mechanism may have failed to detect). Alternate safety mechanisms are typically used when there is no direct test for a safety mechanism.

6.3 Description of Functional Safety Mechanisms

This section provides a brief summary of the functional safety mechanisms available on this component.

6.3.1 Video Path Protection

To prevent against corrupted image, the DLP4620S-Q1 chipset includes many Built-In Self Tests (BISTs) that monitor the video path. The BISTs implemented in the chipset monitor and diagnose the input, the processing, and output of the video. An overview of the entire video path with the BISTs is shown in Figure 6-1 below. Further description of the video path and the BISTs is provided in the following sections.

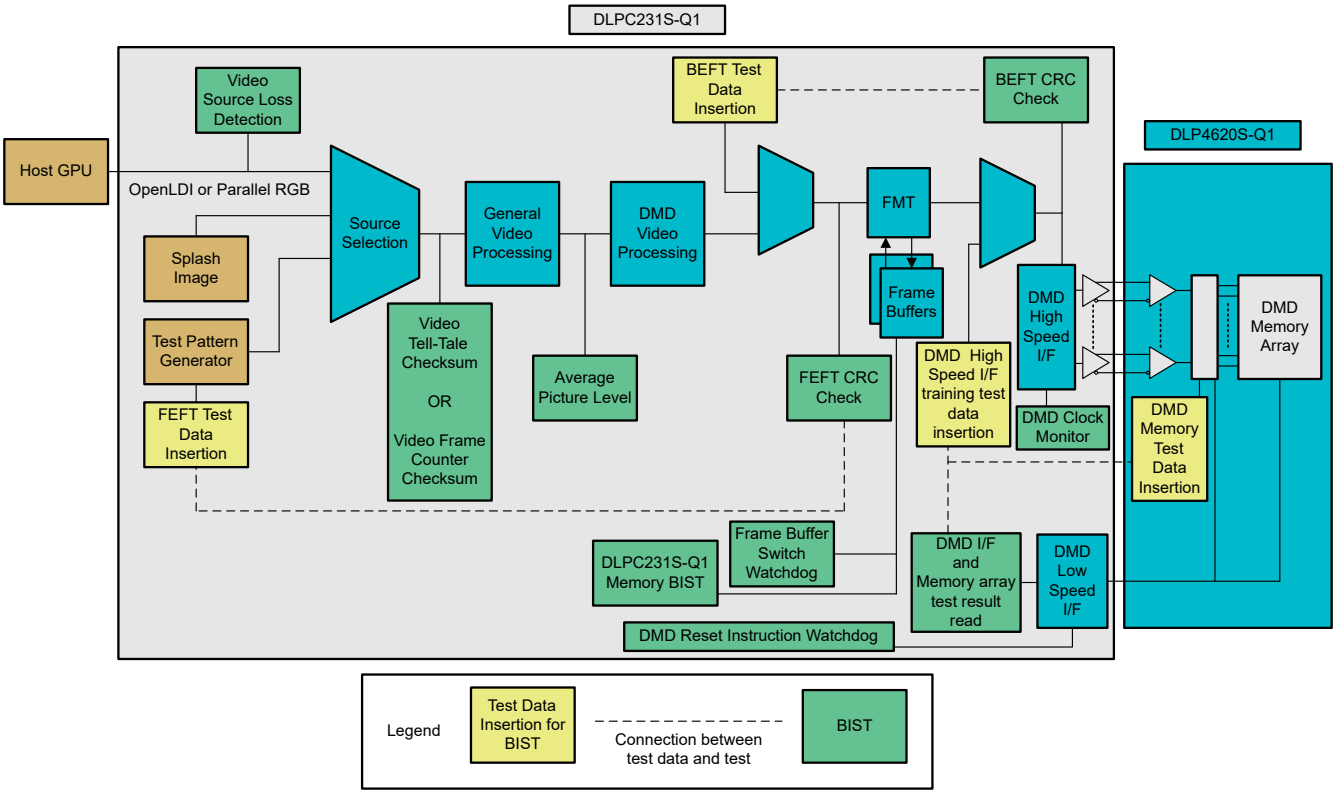

Figure 6-1. DLP4620S-Q1 Video Path With Diagnostics

Figure 6-2 shows the video path of the DLP4620S-Q1 chipset.

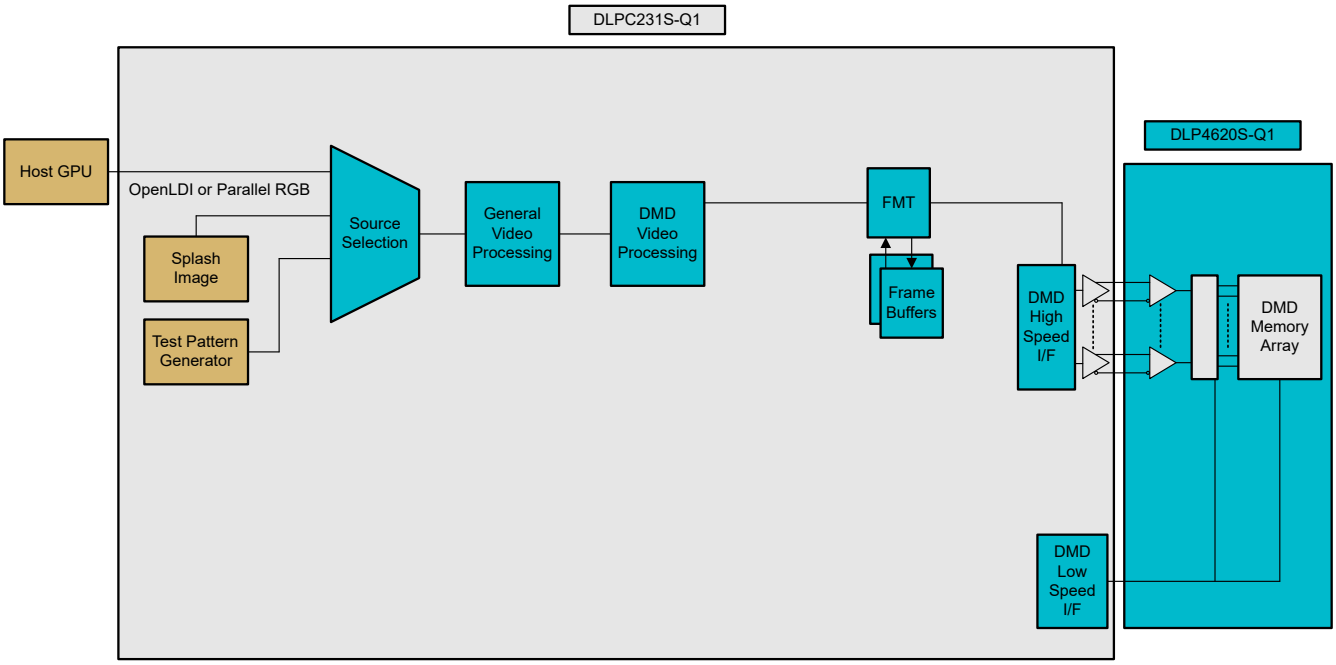

Figure 6-2. DLP4620S-Q1 Video Path

The DLPC231S-Q1 can use several display sources. Source video can come from a vehicle's GPU, either using OpenLDI or Parallel RGB, Internal Test Patterns, or Splash Images. The video source is selected by a host MCU.

After the input multiplexer, some general video processing is applied to the video. This processing includes scaling, and color space correction (for some splash images). Next, some DMD specific video processing is applied. This includes de-gamma correction, dithering, and finally, a conversion to single color "bit plane" data.

"Bit Planes" are sub-frames corresponding to single color codes. The DMD displays single color sub-frames and the human eye integrates them to form a full color image for that frame of the video. After conversion from standard video to bit planes the video is sent to the FMT block.

The FMT consists of some video processing logic and is connected to two frame buffers. The processing in the FMT and the use of the frame buffers is explained below:

- Performs flips, crops, and bezel adjustment of the video. This video is stored into one of the two frame buffers.
- Simultaneously, video from the other frame buffer is output to the DMD.
- The two frame buffers switch roles every frame.

The DMD High Speed Interface is used to load time multiplexed binary data into the DMD's Memory Array. This binary data determines the state of each DMD mirror during each "bit plane". A reset pulse transitions micro-mirrors from one "bit plane" to the next. The DLPC231S-Q1 utilizes a low speed interface that is used for configuration of DMD registers, generating the DMD mirror reset waveforms, and monitoring the DMD.

The DLP4620S-Q1 chipset contains overlapping BIST coverage of the various blocks involved in the video path. These BISTs cover the input, processing, and output of the video path. These BISTs are discussed in the following sections.

6.3.1.1 Video Input BISTs

Figure 6-3 gives an overview of BISTs used to monitor the video input.

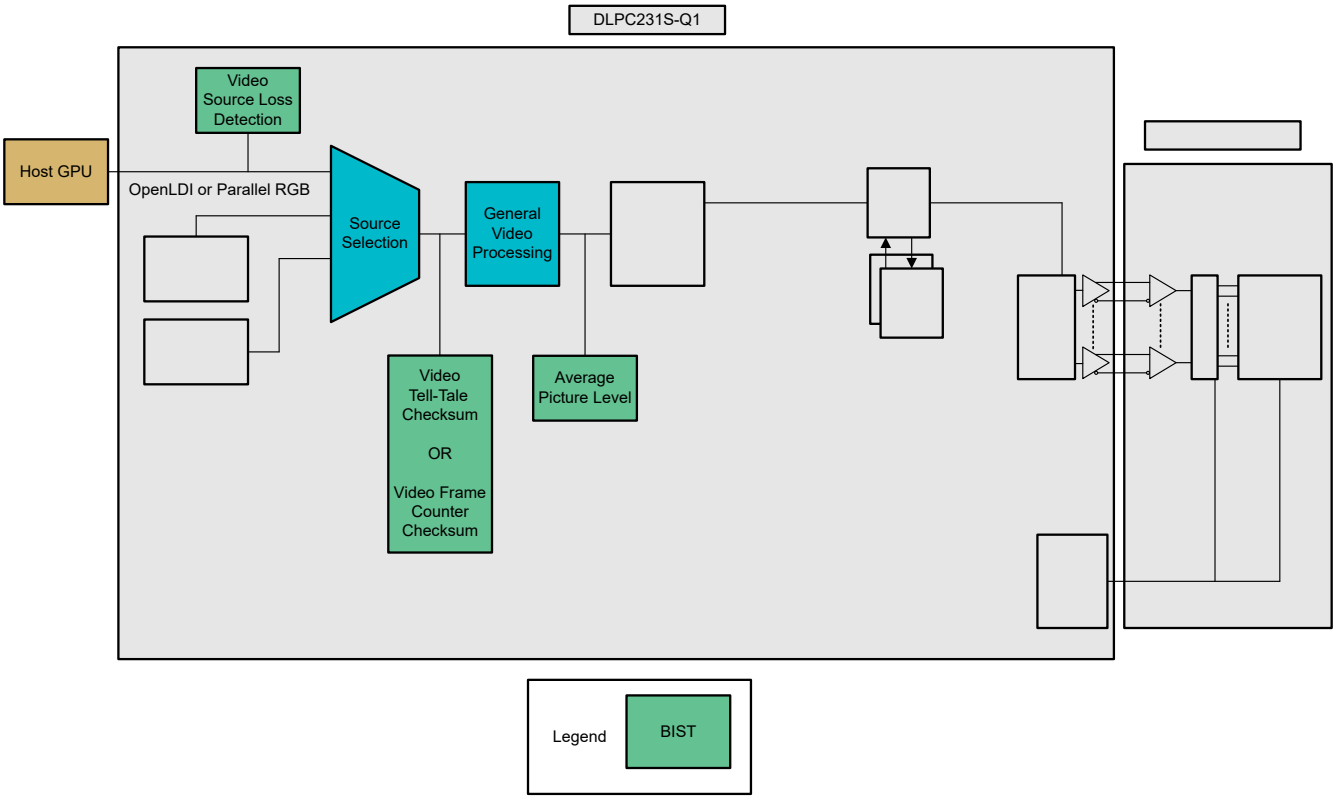

Figure 6-3. Video Input BISTs

- **[SM_1] Video Source Loss Detection:** Checks if the source of video to the DLPC231S-Q1 has disconnected. It checks the video parameters to make sure they are within acceptable ranges. These parameters are the pixel clock frequency, the VSYNC frequency, the number of active lines per frame, and number of active pixels per line. If the video source is invalid at the initial transition to display mode, no image will be displayed. The system will stay in standby mode. If the source becomes invalid after Display Mode operation, the system will transition to an alternate display image specified in the configuration options —either a test pattern or splash image. In some cases it is possible for the system to auto-recover after a source loss. Auto-recover and alternate source settings can be configured in flash.
- **[SM_2] Video Tell-Tale Checksum:** Checks the expected video from the host versus the video received by the DLPC231S-Q1. Host MCU provides a checksum for a region of the image, and the DLPC231S-Q1 calculates a checksum over the same region. If the two checksums don't match, the test fails. This checksum can be performed over any rectangular region of the video, including and up to the entire image. However, this test is designed to be used on static or slowly changing portions of the image. The test region of the checksum and the expected checksum can only be changed while the test is disabled. A minimum of two frames is required to disable the test, update the checksum region and/or value, and re-enable the test. The failure action is configurable in flash, but not during operation. Upon test failure, an error can be logged with no additional action, an error can be logged with a change to an alternate source, or an error can be logged and emergency shutdown can be executed. **This test cannot be used simultaneously with the Video Frame Counter Checksum.**
- **[SM_3] Video Frame Counter Checksum:** Checks the value of a counter embedded within the video data from the host. If the counter does not increment as expected, the test fails. A subsection of the image can be defined as the counter. The minimum and maximum expected value of this counter is also configurable. Once the counter reaches the maximum, it is expected to roll over and start from the minimum. The counter region can be as small as one pixel and as large as the entire image. HUD images typically have large amounts of unused area in the display area. It is recommended to embed the counter in one of these regions, such

as a corner. If the area is sufficiently small, its pixel data can change without being noticeable by the viewer. The failure action is configurable in flash, but not during operation. Upon test failure, an error can be logged with no additional action, an error can be logged with a change to an alternate source, or an error can be logged and emergency shutdown can be executed. **This test cannot be used simultaneously with the Video Tell-Tale Checksum**

- **[SM_4] Average Picture Level:** Checks the numerical average of the incoming pixel data. If the average level is higher than the host specified maximum, the test fails. The failure action is configurable during flash build, but not during operation. Upon test failure, only an error can be logged, or an error can be logged and emergency shutdown can be executed.

6.3.1.2 Video Processing BISTs

Figure 6-4 gives an overview of the BISTs used to monitor and diagnose the video processing blocks in the DLPC231S-Q1.

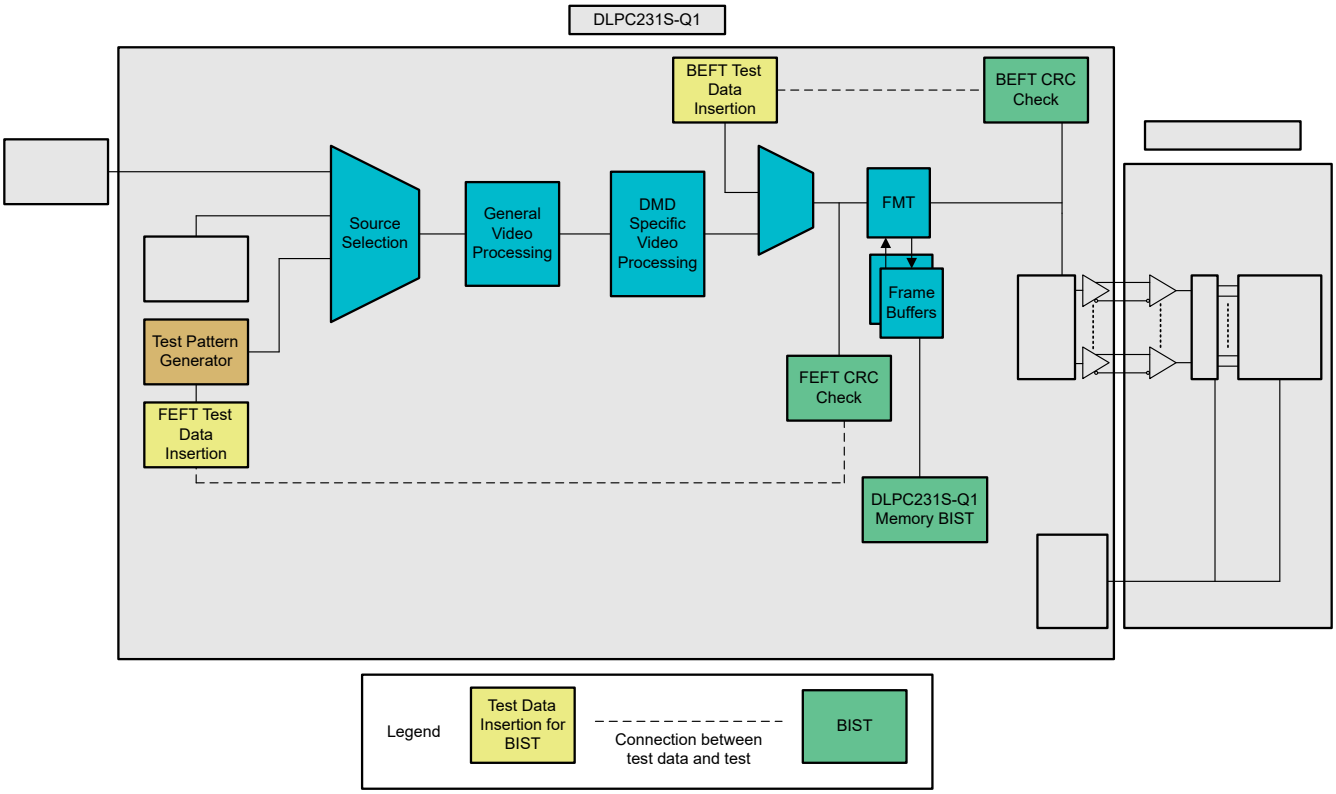

Figure 6-4. Video Processing BIST

- **[SM_5] Front-End Functional Test (FEFT):** Checks the video processing blocks in the DLPC231S-Q1 by inserting a test pattern data and performing a CRC check on the output of processing blocks. The test pattern is a 1920x608 horizontal ramp pattern with an overlaid random noise pattern. The size of the image is chosen in order to provide full coverage of the memory control. Two frames of ~120Hz data are tested. This provides a high source pixel clock frequency, in order to stress internal logic. A subset of the image is used for a CRC check. If the CRC after processing does not match the expected CRC, the test fails. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode via host command. In case of test failure, software will not transition Display Mode even if it is commanded by the host. An error will also be logged.
- **[SM_6] Back-End Functional Test (BEFT):** Checks the DLPC231S-Q1 blocks responsible for outputting data from the frame buffers to the DMD driver. This checks functionality such as image flips, smooth image transition functions, and frame buffer swaps. Additionally, functionality related to the synchronization of the video with LEDs is tested. This will be discussed in more detail in Section 6.3.2. This test checks a 160x60 image with four configurations—no flip, East/West flip only, North/South flip only, and East/West plus North/South flip. The image size is small in order to increase test speed. The goal of this test is not to provide full

coverage of the frame buffers, because that coverage is already provided by other tests. A CRC check is performed on the image after formatting. If the resulting CRC does not match the expected value, the test fails. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode via host command. In case of test failure, software will not transition to Display Mode even if it is commanded by the host. An error will also be logged.

- **[SM_7] DLPC231S-Q1 Memory BIST:** Checks functionality of internal memories such as the frame buffers, internal RAM, and sequence look up tables using a series of writes, delays, and reads. The frame buffer memory check is critical for diagnosing a corrupt video path. The SRAM frame buffers are tested using a series of instructions provided by the manufacturer of the SRAM cell. The instructions for executing the test are stored in external flash, but the test data is generated locally in the frame buffer. If the data read from the memory does not match the data written to the memory the test fails. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode via host command. In case of test failure, software will not transition to Display Mode even if it is commanded by the host. An error will also be logged.

6.3.1.3 Video Output BISTs

Figure 6-5 gives an overview of the BISTs used to monitor and diagnose the video output blocks in the DLP4620S-Q1 chipset.

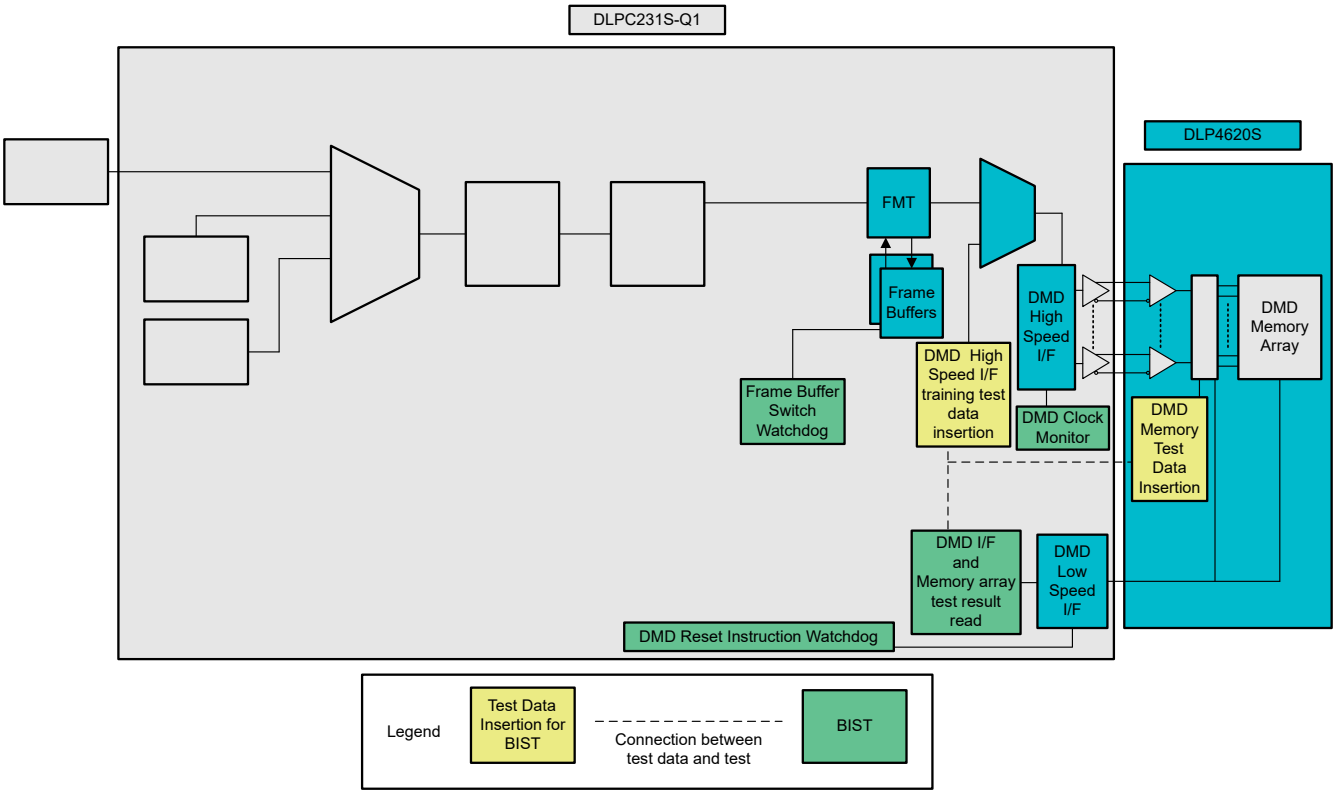

Figure 6-5. Video Output BISTs

- **[SM_8] Frame Buffer Swap Watchdog:** Checks that the frame buffers are switching roles each frame. Each frame, one buffer stores processed video, and the other buffer outputs data to the DMD. If the buffers don't switch each frame, the video will not update. The software of the DLPC231S-Q1 sets a timer for the buffer swap. When the buffer is successfully swapped, a signal from the frame buffer controller resets the timer. If the swap does not happen within the allocated time, the timer will expire. If the timer expires, the test fails. Upon failure, emergency shutdown will be executed and an error will be logged. This test is always active when an external video source or internal test pattern are being used. This test is not executed when a splash image is being displayed.
- **[SM_9] DMD High Speed Interface Training:** The DLPC231S-Q1 to DMD sub-LVDS interface can adjust the phase of each signal in order to optimize the position of the clock signal within the data eye. This process

compensates for variation in manufacturing, system temperature, and drive voltage. This process is called training. This training process can also detect faults in the DLPC231S-Q1 to DMD connection. The DMD low speed interface is used to configure the DMD for training and to read back the results of the training. This training is performed at start-up and continuously during display mode. A total of 8 frames is required to test all data pairs in theDLP4620S-Q1 chipset during display mode. If the test fails at start-up the system will stay in Stand-By mode, and an error will be logged. If failure happens during display mode, an error is logged. During display mode, failures may be transient. However, persistent errors can indicate a broken connection or another critical issue.

- **[SM_10] DMD Low Speed Interface Test:** Checks the DMD low speed interface by continuously writing a dedicated register and reading back the value. Reads and writes happen simultaneously with DMD High Speed Training Cycles. The DMD Low Speed Interface Test takes four total training cycles. A value is written in cycle 0, read back in cycle 1, the 1-s complement value is written in cycle 2, and another read is performed in cycle 3. This test is always executed during display mode. Upon failure, an error is logged.
- **[SM_11] DMD Memory Test:** Checks the DMD CMOS memory by writing data and confirming read back data. The DLPC231S-Q1 commands the DMD into a testing mode and the DMD writes known values into the memory cells below its pixels. The DMD then reads back the state of each memory cell and drives a signal to the DLPC231S-Q1 to indicate pass or fail for each column of the DMD memory. A column will be reported as a fail if one or more memory cells in that column reads an incorrect value. If a failure is detected in more than one column, the test fails. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode via host command. In case of test failure, software will not transition Display Mode even if it is commanded by the host. An error will also be logged.
- **[SM_12] DMD Reset Instruction Watchdog:** Checks that the DMD has accepted command to update mirror positions. A reset command from the DLPC231S-Q1 tells the DMD to update mirror positions. If this command is not executed, mirrors will remain in their current position. Upon successfully receiving a reset command the DMD returns an acknowledge message. If this is not received by the DLPC231S-Q1 within an acceptable time, this test fails. Upon failure, emergency shutdown will be executed and an error will be logged. This test is always active when an image is being displayed.
- **[SM_13] DMD Clock Monitor:** The DLPC231S-Q1 clock generation block contains monitoring to ensure that the clock frequency of the DMD high speed interface is within the specified range.

6.3.2 Illumination Control Protection

The LEDs in the system should be properly controlled to prevent a bright image. In cases where proper control is not possible, the illumination should be turned off.

The DLP4620S-Q1 chipset includes several features to monitoring the illumination control and turn off the LEDs in case of a fault.

Figure 6-6 and Figure 6-7 show the illumination control and LED driver architecture. Figure 6-8 shows the origin and destination of software, data, and settings.

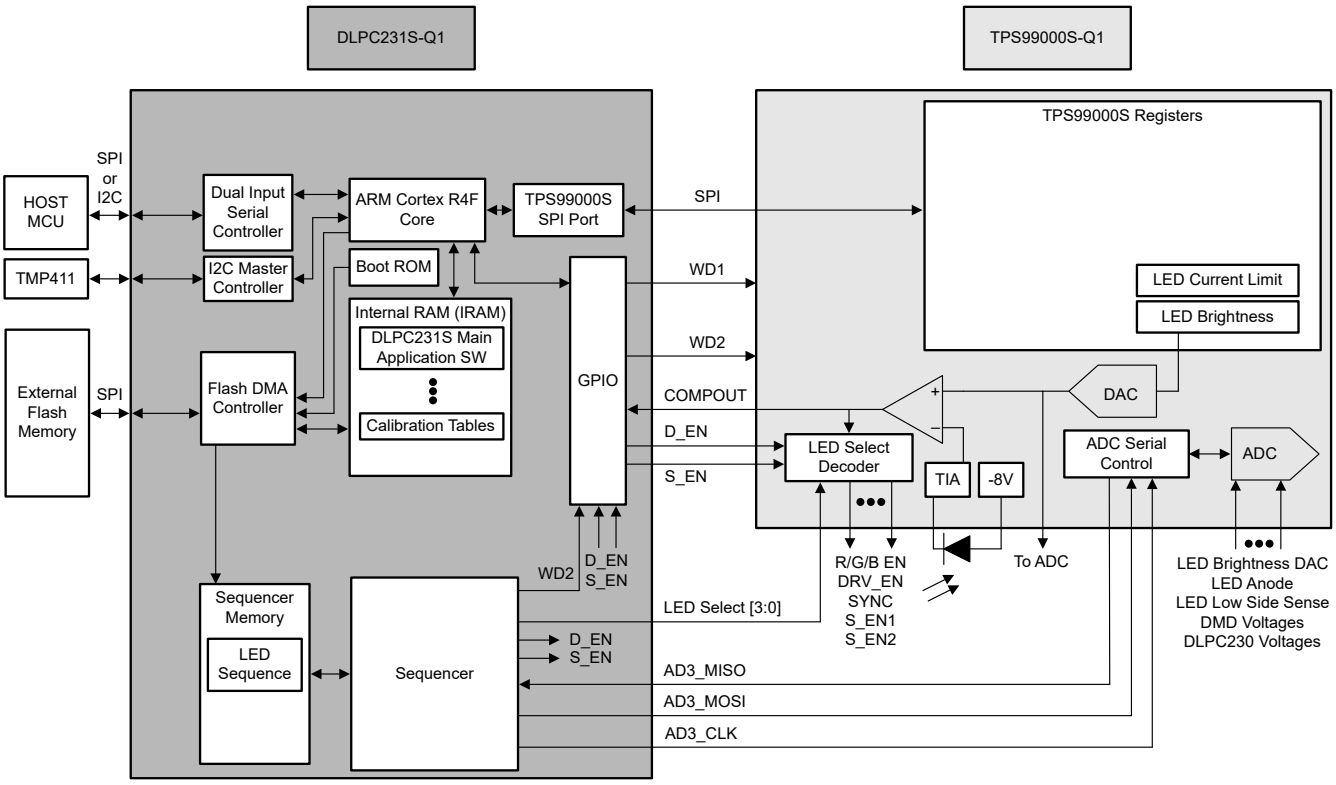

Figure 6-6. Illumination Control Architecture

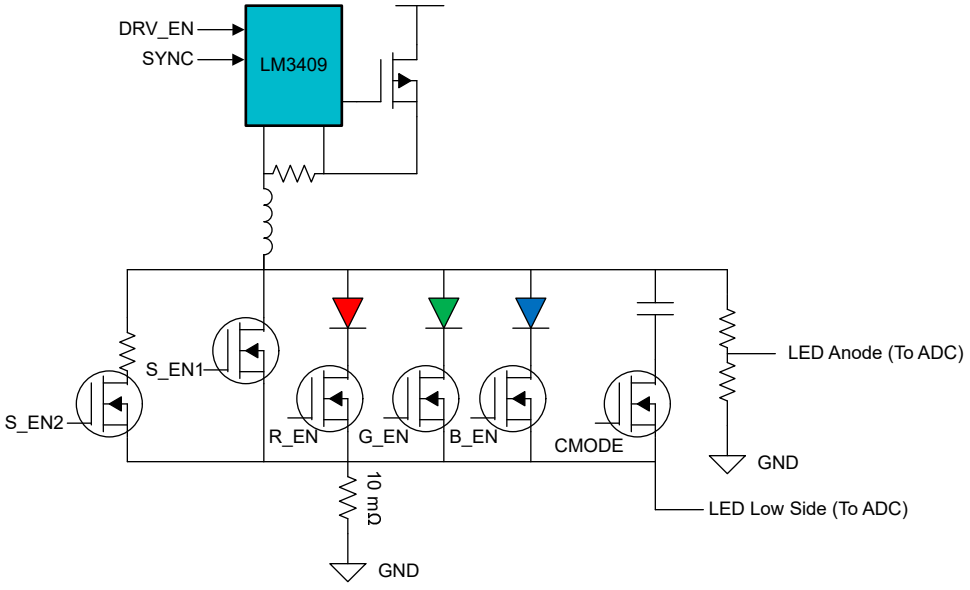

Figure 6-7. LED Driver Architecture

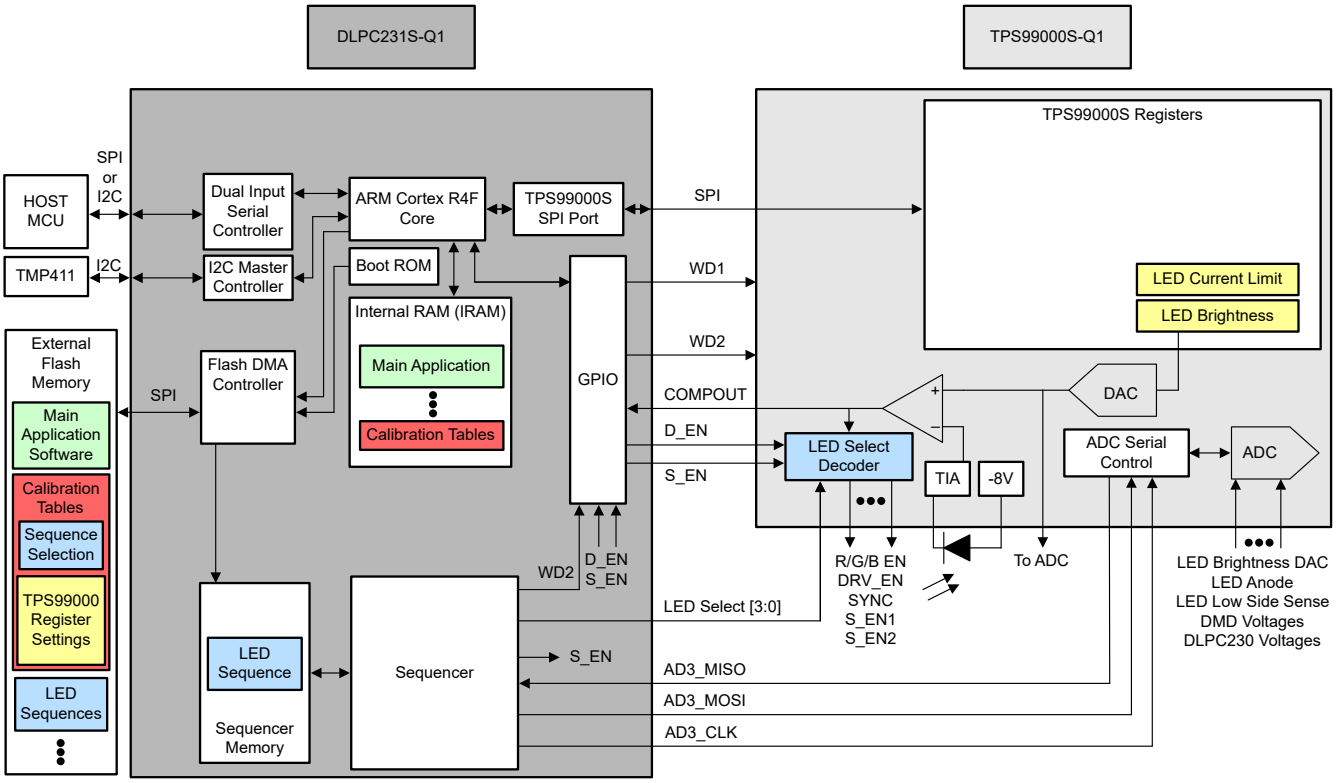

Figure 6-8. Software and Settings Origin and Destination

As seen in Figure 6-6, Figure 6-7, and Figure 6-8:

- At start-up, the Boot ROM commands External Flash to load the Main Application Software and calibration data into the internal RAM (IRAM) of the DLPC231S-Q1. The ARM Core in the DLPC231S-Q1 executes the main application loaded in to the IRAM.
- The host MCU sends dimming commands periodically to the DLPC231S-Q1 to specify the brightness level of the system. At start-up, the calibration data provides a default dimming level.
- Based on the dimming level and calibration data, the DLPC231S-Q1 Software determines the correct LED sequence and TPS99000S-Q1 register settings. The LED sequence is the order and timing of LED pulses. TPS99000S-Q1 register settings determine the brightness of the LED pulses.
- The LED sequence determined by calibration data is requested to be loaded from external flash to the sequencer memory. The sequencer block uses the sequence loaded into its memory to send LED select signals to the TPS99000S-Q1. These signals control the enable and disable for individual LEDs.
- LED brightness is regulated to the level requested by the DLPC231S-Q1 via a feedback loop consisting of the TPS99000S-Q1, LM3409, the LEDs, and a photo-diode. The brightness target is set by the DLPC231S-Q1 into a DAC in the TPS99000S-Q1. LED brightness is measured by a photo-diode and trans-impedance amplifier (TIA) inside the TPS99000S-Q1. The target brightness and the measured brightness are compared by a comparator in the TPS99000S-Q1. The output of the comparator is used for hysteretic control of the LED light level.

Figure 6-9 shows an overview of all of the monitoring and diagnostics BISTs included in the DLP4620S-Q1 chipset.

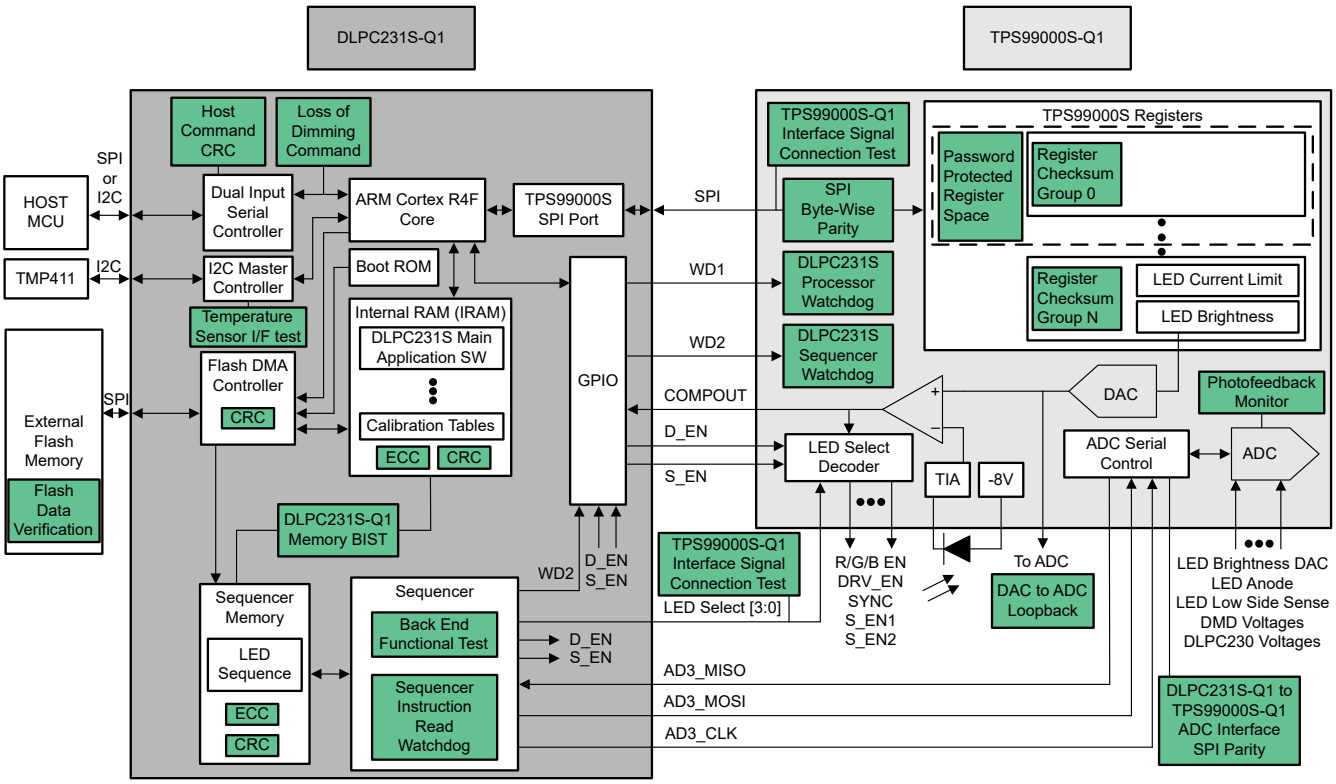

Figure 6-9. Illumination Control Architecture With Diagnostics

6.3.2.1 Communication Interface and Register Protection

The following methods are used to protect communication between ICs in the system and the data stored in critical registers.

- **[SM_14] Host Command CRC:** A CRC check on the incoming host commands to detect corrupted commands. Protects against incorrect dimming value being set due to a corrupted command.
- **[SM_15] Loss Of Dimming Command Test:** Checks that dimming commands are regularly being received from the host. This enures that communication with the host has not been lost. If communication with the host is lost, and old dimming value may create an image that is too bright for the current driving conditions. The host can configure a timer within which the DLPC231S-Q1 should receive a dimming command. If the command is not received within this timing the test fails. A default value for the timer can also be configured in flash. Upon failure, emergency shutdown will be executed and an error will be logged.
- **[SM_16] TPS99000S-Q1 Interface Signal Connection Test:** Checks the SPI and the LED select interfaces between theDLPC231S-Q1 and TPS99000S-Q1. Checks SPI interface by writing to a dedicated register and reading back the value. Checks the LED select interface by sending LED select signals and reading back the LED select values from the TPS99000S-Q1 via SPI. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode via host command. Upon failure, software will not transition Display Mode even if it is commanded by the host. An error will also be logged.
- **[SM_17] DLPC231S-Q1 to TPS99000S-Q1 SPI Byte-Wise Parity:** The DLPC231S-Q1 to TPS99000S-Q1 SPI interface implements a byte-wise parity for detecting command or data corruption. The DLPC231S-Q1 sends a parity bit with the payload for any read or write from the TPS99000S-Q1 registers. If the TPS99000S-Q1 detects a parity error it will indicate a parity error to the DLPC231S-Q1 via a status bit. Register writes to the TPS99000S-Q1 will not be performed if a parity error is detected. If the DLPC231S-Q1 detects three consecutive frames of parity error, it will not reset the DLPC231S-Q1 Processor Watchdog Timer (WD1). This will result in an emergency shutdown. An error code will also be logged.
- **[SM_18] DLPC231S-Q1 to TPS99000S-Q1 ADC Interface SPI Parity:** The DLPC231S-Q1 to TPS99000S-Q1 implements a parity check to ensure that ADC measurement commands and data are not corrupted.

Parity is implemented on both the read command transaction and on the return data. Each command transaction from the DLPC231S-Q1 to TPS99000S-Q1 includes a start bit, the command id, the command id repeated, a parity bit, and a stop bit. The repeated command and data bytes must match and the parity bit must be correct. Additionally, the data returned from the TPS99000S-Q1 to DLPC231S-Q1 includes 12 data bits, 3 error bits, 12 data bits repeated, 3 error bits repeated, and 1 parity bit. The two copies of the 12-bit data, and the two copies of the 3-bit error codes must match. Additionally, the parity bit must be correct. If the TPS99000S-Q1 detects a parity error, it will indicate the error to the DLPC231S-Q1 via a status bit. If 3 consecutive errors are detected, the test fails. Upon failure, emergency shutdown will be executed and an error will be logged.

- **[SM_19] TPS99000S-Q1 Password Protected Register Space:** A portion of the TPS99000S-Q1 register space is protected by a password. The DLPC231S-Q1 unlocks this register space by writing the password before updating these registers. After updating these registers, the DLPC231S-Q1 locks this register space.
- **[SM_20] TPS99000S-Q1 Register Checksum:** The TPS99000S-Q1 implements a checksum on functionally grouped registers. This checksum is used to detect bit level changes occurring due to random events. When the DLPC231S-Q1 updates any TPS99000S-Q1 registers, it updates the checksum for that group. The TPS99000S-Q1 periodically calculates a checksum on each group of registers and compares it to the last checksum stored by the DLPC231S-Q1. If the TPS99000S-Q1 detects a checksum error, it sets a status bit that can be read by the DLPC231S-Q1 via SPI. If an error is detected, the DLPC231S-Q1 will attempt to re-write the registers and checksum up to three times. If the error persists after three attempts, an emergency shutdown will be executed and an error will be logged.

6.3.2.2 LED Control Feedback Loop Protection

The following methods are used to monitor and diagnose the control the LED control and feedback loop:

- **[SM_21] DAC to ADC Loopback Test:** Checks that the ADCs and DACs used to regulated LED brightness and current limit are functioning properly. Sets DAC levels and then measures the output of the DAC via ADC. If the ADC measurements do not match the expected DAC levels, the test fails. This test can be configured to run at start-up and it can be executed by command after the software is changed to Stand-by mode using the host command. Upon failure, software will not transition to Display Mode even if it is commanded by the host. An error will also be logged.
- **[SM_22] Photo Feedback Monitor:** Checks the connection of the photodiode used to regulate LED brightness. The disconnection of the photodiode could result in a very bright image. The DLP4620S-Q1 chipset has two modes of operation—continuous mode for high brightness and discontinuous mode for mid and low brightness. In continuous mode, this test compares the output of the photodiode amplifier versus the LED current. A high LED current and low photodiode reading on for all LEDs indicates that the photodiode is disconnected. In discontinuous mode, LED current measurements are not possible, so a different method is used. The COMPOUT signal indicates whether the photodiode measurement is below or above the target brightness level of the LEDs. If the photodiode measurement never reaches the target LED brightness for all LEDs in one frame, the photodiode is considered disconnected. To prevent false failures, the number of consecutive frames that the error must persist for it to be considered a real failure is configurable in flash. The number of frames can be increased for preventing false failures. However, the number of frames needed to indicate an error and respond to it should be less than the Fault Tolerant Time Interval (FTTI) specified by the OEM. Upon failure, emergency shutdown will be executed and an error will be logged. This test is always executed during display mode.
- **[SM_6] Back End Functional Test (BEFT):** Tests the sequencer block by executing a specialized LED sequence, but without turning on LEDs. Tests the sequencer block's ability to access and execute commands from sequencer memory. Makes sure that the sequencer can properly control LED illumination signals in continuous and discontinuous mode. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode using the host command. In case of test failure, software will not transition to Display Mode even if it is commanded by the host. An error will also be logged.

6.3.2.3 Data Load and Transfer Protection

The DLPC231S-Q1 contains several internal memories, such as the internal RAM and the sequencer memory. Data loaded into these memories comes from the external flash. The Flash Direct Memory Access (FDMA) block is used to facilitate the access and transport of data to the proper memories. To prevent or detect corruption of this data, the following features are implemented in the DLPC231S-Q1:

- **[SM_23] Flash Table Transport CRC:** The DLPC231S-Q1 performs two CRC checks on all data that is transported from flash to internal memories such as IRAM and sequencer memory. When the data is originally generated, a CRC is calculated and appended to each block. When data is loaded from flash to an internal memory, the embedded software reads the expected CRC value from flash. Next, the FDMA block calculates a CRC as the data is transferred. This CRC is compared to the expected CRC. Lastly, another CRC is calculated by the destination memory (IRAM, sequencer memory, etc.) hardware. If the CRCs do not match at any point, the data will be re-loaded and an error will be logged.
- **[SM_24] ECC:** The internal memories of the DLPC231S-Q1 implement ECC. The ECC can correct single-bit errors and detect, but not correct, multi-bit errors. In case of any errors, an error will be logged. In case of multi-bit errors an emergency shutdown will be executed.
- **[SM_25] DLPC231S-Q1 Memory BIST:** Checks functionality of internal memories such as the frame buffers, internal RAM, and sequence look up tables using a series of writes, delays, and reads. The frame buffer memory check is critical for diagnosing a corrupt video path. The SRAM frame buffers are tested using a series of instructions provided by the manufacturer of the SRAM cell. The instructions for executing the test are stored in external flash, but the test data is generated locally in the frame buffer. If the data read from the memory does not match the data written to the memory the test fails. This test can be configured to run at start-up, and it can be executed by command after the software is changed to Stand-by mode using the host command. In case of test failure, software will not transition Display Mode even if it is commanded by the host. An error will also be logged.
- **[SM_26] Flash Data Verification:** Each block of flash data contains an expected CRC. The DLPC231S-Q1 software calculates the CRC of each block and compares it to the expected CRC stored in flash. If there is a mismatch, the test fails. This test is typically executed after programming flash data. A flash option determines if this test is executed at start-up. TI recommends enabling this option. This test can also be executed from standby mode. In case of failure, software will not transition Display Mode even if it is commanded by the host. An error will also be logged.
- **[SM_27] Periodic Refresh:** Memories in the DLPC231S-Q1 video path are periodically refreshed. For example, the frame buffers are reloaded every frame. The short reload period of these refreshes compared to the fault tolerant time interval means that the periodic refresh can be considered as a safety mechanism against transient errors in memories. Periodic refresh does not protect against permanent faults.
- **[SM_28] Boot ROM CRC:** The boot application runs a CRC on the boot ROM data and compares it to an expected value stored in the boot ROM memory. If the CRCs do not match, the test fails. Upon failure, the failure stays in the boot application and does not proceed and logs an error.

6.3.2.4 Watchdogs and Clock Monitors

The following watchdogs are used to monitor that the various blocks of the DLPC231S-Q1 are properly operating. This is critical to ensuring that the LED brightness levels and timings are being properly controlled.

- **[SM_29] TPS99000S-Q1 Clock Ratio Monitor:** The TPS99000S-Q1 calculates the ratio between its internal clock and the external DLPC231S-Q1 clock input in order to validate proper frequency operation of the main DLPC231S-Q1 clock source. The DLPC231S-Q1 main application periodically reads this ratio. If the ratio is outside of the expected range, the test fails. Upon failure an error is logged.
- **[SM_30] DLPC231S-Q1 Processor Watchdog (WD1):** The TPS99000S-Q1 monitors the DLPC231S-Q1 processor to make sure that it is continuously operating. The main application software periodically resets the watchdog timer within an allocated time window. If the watchdog signal is not received by the TPS99000S-Q1 during the time window, the test fails. Upon failure, the TPS99000S-Q1 will signal a park of the DMD and reset the chipset. The main application will read the reset cause from the TPS99000S-Q1 and assert HOST_IRQ during reset initialization.
- **[SM_31] DLPC231S-Q1 Sequencer Watchdog (WD2):** The TPS99000S-Q1 monitors the SEQ_START signal that is generated by the sequencer at the beginning of each frame. If the signal is not received within approximately 7 frames, the TPS99000S-Q1 determines that the sequencer is not functioning properly. The TPS99000S-Q1 alerts the DLPC231S-Q1. The DLPC231S-Q1 will attempt to disable and re-enable the sequencer 3 times. If it is unsuccessful after 3 tries, and emergency shutdown will be executed and an error will be logged.
- **[SM_32] Sequencer Instruction Read Watchdog:** During proper operation, the sequencer block constantly reads and executes instructions from the sequencer memory. The main application software sets a timer within which an instruction must be read from memory. The timer is reset every time an instruction is read.

If an instruction is not read within the allocated time, the test fails. Upon failure, emergency shutdown will be executed and an error will be logged. This test is always active when an image is being displayed.

- **[SM_12] DMD Reset Instruction Watchdog:** Checks that the DMD has accepted command to update mirror positions. A reset command from the DLPC231S-Q1 tells the DMD to update mirror positions. If this command is not executed, mirrors will remain in their current position. Upon successfully receiving a reset command the DMD returns an acknowledge message. If this is not received by the DLPC231S-Q1 within an acceptable time, this test fails. Upon failure, emergency shutdown will be executed and an error will be logged. This test is always active when an image is being displayed.

6.3.2.5 Voltage Monitors

The following voltage monitors are used to make sure that the device operating voltages of the chipset are within an acceptable range

- **[SM_33] TPS99000S-Q1DLPC231S-Q1 Real-Time Voltage Monitors:**: The TPS99000S-Q1 monitors the 1.1V, 1.8V, and 3.3V power supplies to the DLPC231S-Q1. These voltages are not generated by the TPS99000S-Q1. If any these voltages drop below the thresholds specified in the TPS99000S-Q1 datasheet, the TPS99000S-Q1 asserts the PARK_Z signal low. This initiates a hardware park routine within the DLPC231S-Q1, meaning no software is executed in order for this routine to execute. The hardware park routine disables LEDs and video output to the DMD. After the routine is completed, the TPS99000S-Q1 asserts RESET_Z low, which puts the DLPC231S-Q1 into reset.
- **[SM_34] TPS99000S-Q1 DMD Voltage Monitors:**The TPS99000S-Q1 generates and monitors the DMD VOFFSET, VBIAS, and VRESET voltages. Hardware monitors within the TPS99000S-Q1 detect if these voltages are outside the acceptable range and assert the PARK_Z signal low. This initiates a hardware park routine within the DLPC231S-Q1, meaning no software is executed in order for this routine to execute. The hardware park routine disables LEDs and video output to the DMD. After the routine is completed, the TPS99000S-Q1 asserts RESET_Z low, which puts the DLPC231S-Q1 into reset.
- **[SM_35] TPS99000S-Q1 Input Voltage Monitor:** The TPS99000S-Q1 monitors the VMAIN input to the system via a voltage divider, AVDD 3.3V input to the TPS99000S-Q1, and the nominal 6V inputs to the TPS99000S-Q1 (VIN_DRST, VIN_LDOT_5V, VIN_LDOA_3P3V, VIN_LDOT_3P3V, DRVR_PWR). If any of these voltages drops below the threshold, the TPS99000S-Q1 asserts PARK_Z signal low. This initiates a hardware park routine within the DLPC231S-Q1, meaning no software is executed in order for this routine to execute. The hardware park routine disables LEDs and video output to the DMD. After the routine is completed, the TPS99000S-Q1 asserts RESET_Z low, which puts the DLPC231S-Q1 into reset.
- **[SM_36] TPS99000S-Q1 Internally Generated Voltage Monitors:**The TPS99000S-Q1 generates and monitors several internally generated voltages (3V for ADCs and TIAs, and -8V for the photo-diode reverse biasing). Hardware monitors within the TPS99000S-Q1 detect if these voltages are outside the acceptable range and assert the PARK_Z signal low. This initiates a hardware park routine within the DLPC231S-Q1, meaning no software is executed in order for this routine to execute. The hardware park routine disables LEDs and video output to the DMD. After the routine is completed, the TPS99000S-Q1 asserts RESET_Z low, which puts the DLPC231S-Q1 into reset.
- **[SM_37] DLPC231S-Q1 DMD Voltage Monitor:** Every video frame the main application takes ADC measurements of the DMD voltages—VOFFSET, VBIAS, and VRESET. If these are not within the acceptable range, and error is logged and emergency shutdown is executed.
- **[SM_38] DLPC231S-Q1 System Voltage Monitor:** Every video frame the main application takes ADC measurements of several system voltages. These include the DLPC231S-Q1 voltages (P1P1V, P1P8V, P3P3V), TPS99000S-Q1 voltages (DVDD, ADC_VREF, LDOT_M8, DRVR_PWR), and VMAIN. The thresholds for VMAIN are flash configurable. Upon failure, an error is logged.

A Summary of Recommended Functional Safety Mechanism Usage

Table A-2 summarizes the functional safety mechanisms present in hardware or recommend for implementation in software or at the system level as described in Section 5. Table A-1 describes each column in Table A-2 and gives examples of what content could appear in each cell.

Table A-1. Legend of Functional Safety Mechanisms

Functional Safety Mechanism	Description
TI Safety Mechanism Unique Identifier	A unique identifier assigned to this safety mechanism for easier tracking.
Safety Mechanism Name	The full name of this safety mechanism.
Safety Mechanism Category	**Safety Mechanism** - This test provides coverage for faults on the primary function. It may also provide coverage on another safety mechanism. **Test for Safety Mechanism** - This test provides coverage for faults of a safety mechanism only. It does not provide coverage on the primary function. **Fault Avoidance** - This is typically a feature used to improve the effectiveness of a related safety mechanism.
Safety Mechanism Type	Can be either hardware, software, a combination of both hardware and software, or system. See Section 6.2 for more details.
Safety Mechanism Operation Interval	The timing behavior of the safety mechanism with respect to the test interval defined for a functional safety requirement / functional safety goal. Can be either continuous, or on-demand. **Continuous** - the safety mechanism constantly monitors the hardware-under-test for a failure condition. **Periodic or On-Demand** - the safety mechanism is executed periodically, when demanded by the application. This includes Built-In Self-Tests that are executed one time per drive cycle or once every few hours.
Test Execution Time	Time period required for the safety mechanism to complete, not including error reporting time. Note: Certain parameters are not set until there is a concrete implementation in a specific component. When component specific information is required, the component data sheet should be referenced. Note: For software-driven tests, the majority contribution of the Test Execution Time is often software implementation-dependent.
Action on Detected Fault	The response that this safety mechanism takes when an error is detected. Note: For software-driven tests, the Action on Detected Fault may depend on software implementation.
Time to Report	Typical time required for safety mechanism to indicate a detected fault to the system. Note: For software-driven tests, the majority contribution of the Time to Report is often software implementation-dependent.

Table A-2. Summary of Functional Safety Mechanisms

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Operation Interval	Test Execution Time	Time to Report	Action on Detected Fault
SM_1	**Video Source Loss Detection**	1 Video Frame	1 Video Frame	5ms	Stay in standby or switch to alternate source

Table A-2. Summary of Functional Safety Mechanisms (continued)

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Operation Interval	Test Execution Time	Time to Report	Action on Detected Fault
SM_2	**Video Tell-Tale Checksum**	1 Video Frame	1 Video Frame	5ms	Configurable: • No Action (Information only) • Log Error and Switch to Alternate Source • Emergency Shutdown and Log Error
SM_3	**Video Frame Counter Checksum**	1 Video Frame	1 Video Frame	5ms	Configurable: • No Action (Information only) • Log Error and Switch to Alternate Source • Emergency Shutdown and Log Error
SM_4	**Average Picture Level**	1 Video Frame	1 Video Frame	1ms or 5ms	Configurable: • Log Error • Emergency Shutdown and Log Error
SM_5	**Front-End Functional Test**	1 Driving Cycle	33ms	1ms	Stay in standby and log error
SM_6	**Back-End Functional Test**	1 Driving Cycle	16ms	1ms	Stay in standby and log error
SM_7	**DLPC231S-Q1 Memory BIST**	1 Driving Cycle	47ms	1ms	Stay in standby and log error
SM_8	**Frame Buffer Switch Watchdog**	1 Video Frame	9x Video Frame	5ms	Emergency shutdown and Log Error
SM_9	**DMD High Speed Interface Training**	1 Video Frame	8x Video Frame	1ms	Log Error
SM_10	**DMD Low Speed Interface Test**	1 Video Frame	1 Video Frame	1ms	Log Error
SM_11	**DMD Memory Test**	1 Driving Cycle	21ms	1ms	Stay in standby and log error
SM_12	**DMD Reset Instruction Watchdog**	1 DMD Mirror Transition Interval	9x Video Frame	5ms	Emergency shutdown and log error
SM_13	**DMD Clock Monitor**	1 Video Frame	1 Video Frame	5ms	Emergency shutdown and log error
SM_14	**Host Command CRC**	1 Host SPI Command Transaction	1 SPI Command Time. Timing depends on SPI frequency	1ms	Log Error

Table A-2. Summary of Functional Safety Mechanisms (continued)

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Operation Interval	Test Execution Time	Time to Report	Action on Detected Fault
SM_15	**Loss of Dimming Command Test**	Software Configurable	Software Configurable	5ms	Emergency shutdown and log error
SM_16	**TPS99000S-Q1 Interface Signal Connection Test**	1 Driving Cycle	3ms	1ms	Stay in standby and log error
SM_17	**DLPC231S-Q1 to TPS99000S-Q1 SPI Byte-Wise Parity**	1 DLPC231S-Q1 to TPS99000S-Q1 command transaction	1.1µs (4 SPI packet transactions at 30MHz; initial transaction + three re-tries)	5ms	Emergency Shutdown and Log Error
SM_18	**DLPC231S-Q1 to TPS99000S-Q1 ADC Interface SPI Parity**	1 DLPC231S-Q1 to TPS99000S-Q1 AD3 transaction	4.1µs (4 transactions at 30MHz; initial transaction + three re-tries)	5ms	Emergency Shutdown and Log Error
SM_19	**TPS99000S-Q1 Password Protected Register Space**	1 DLPC231S-Q1Q1 to TPS99000S-Q1 Register Write	4x Video Frame	N/A	No failure action. TPS99000S-Q1 Register Checksum would likely indicate if there was a failure during the password protection.
SM_20	**TPS99000S-Q1 Register Checksum**	1 Video Frame	1 video frame to detect and correct 4 video frames to detect persistent error	5ms	Emergency Shutdown and Log Error
SM_21	**DAC to ADC Loopback Test**	1 Driving Cycle	27ms	1ms	Stay in standby and log error
SM_22	**Photo Feedback Monitor**	1 Video Frame	Software Configurable	5ms or 1ms	Depends on failure condition: • Emergency Shutdown and Log Error • Log Error
SM_23	**Flash Table Transport CRC**	Every Data Transfer from Flash	1 Video Frame	1ms	Re-load data and Log Error
SM_24	**DLPC231S-Q1 Memory ECC**	Continuous		1ms or 5ms	• Correct Single-Bit Errors and Log Error • Emergency Shutdown and Log Error for multi-bit error
SM_25	**DLPC231S-Q1 Memory BIST**	1 Driving Cycle			Stay in standby and log error
SM_26	**Flash Data Verification**	1 Driving Cycle	42µs / Kbyte of flash data	1ms	Stay in standby and log error
SM_27	**Periodic Refresh**	1 Video Frame or less	N/A	N/A	N/A
SM_28	**Boot ROM CRC**	1 Driving Cycle	N/A	N/A	Stay in boot and log error
SM_29	**TPS99000S-Q1 Clock Ratio Monitor**	1 Video Frame	1 Video Frame		Log error

Table A-2. Summary of Functional Safety Mechanisms (continued)

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Operation Interval	Test Execution Time	Time to Report	Action on Detected Fault
SM_30	**DLPC231S-Q1 Processor Watchdog (WD1)**	72ms	128ms	5ms	HOST_IRQ and system reset
SM_31	**DLPC231S-Q1 Sequencer Watchdog (WD2)**	1 Video Frame	7x Video Frame	5ms	Emergency Shutdown and Log Error
SM_32	**Sequencer Instruction Read Watchdog**	Every sequencer instruction read, typically < 200µs	9x Video Frame	5ms	Emergency Shutdown and Log Error
SM_33	**TPS99000S-Q1DLPC231S-Q1 Real-Time Voltage Monitors**	Continuous	52µs	<17ms	Emergency Shutdown
SM_34	**TPS99000S-Q1 DMD Voltage Monitors**	Continuous	52µs	<17ms	Emergency Shutdown
SM_35	**TPS99000S-Q1 Input Voltage Monitor**	Continuous	52µs	<17ms	Emergency Shutdown
SM_36	**TPS99000S-Q1 Internally Generated Voltage Monitors**	Continuous	Immediately	<17ms	Emergency Shutdown
SM_37	**DLPC231S-Q1 DMD Voltage Monitor**	1 Video Frame	1 Video Frame	5ms	Emergency Shutdown and Log Error
SM_38	**DLPC231S-Q1 System Voltage Monitor**	1 Video Frame	1 Video Frame	1ms	Log Error

B Distributed Developments

A Development Interface Agreement (DIA) is intended to capture the agreement between two parties towards the management of each party's responsibilities related to the development of a functional safety system. TI functional safety components are typically designed for many different systems and are considered to be Safety Elements out of Context (SEooC) hardware components. The system integrator is then responsible for taking the information provided in the hardware component safety manual, safety analysis report and safety report to perform system integration activities. Because there is no distribution of development activities, TI does not accept DIAs with system integrators.

TI functional safety components are products that TI represents, promotes or markets as helping customers mitigate functional safety related risks in an end application and/or as compliant with an industry functional safety standard or FS-QM. For more information about TI functional safety components, go to TI.com/functionalsafety.

B.1 How the Functional Safety Lifecycle Applies to TI Functional Safety Products

TI has tailored the functional safety lifecycles of ISO 26262 and IEC 61508 to best match the needs of a functional Safety Element out of Context (SEooC) development. The functional safety standards are written in the context of the functional safety systems, which means that some requirements only apply at the system level. Since TI functional safety components are hardware or software components, TI has tailored the functional safety activities to create new product development processes for hardware and for software that makes sure state-of-the-art techniques and measures are applied as appropriate. These new product development processes have been certified by third-party functional safety experts. To find these certifications, go to TI.com/functionalsafety.

B.2 Activities Performed by Texas Instruments

The TI functional safety products are hardware components developed as functional Safety Elements out of Context. As such, TI's functional safety activities focus on those related to management of functional safety around hardware component development. System level architecture, design, and functional safety analysis are not within the scope of TI activities and are the responsibility of the customer. Some techniques for integrating the SEooC safety analysis of this hardware component into the system level can be found in ISO 26262-11.

Table B-1. Activities Performed by Texas Instruments versus Performed by the customer

Functional Safety Lifecycle Activity[1]	TI Execution	Customer Execution
Management of functional safety	Yes	Yes
Definition of end equipment and item	No	Yes
Hazard analysis and risk assessment (of end equipment/ item)	No	Yes
Creation of end equipment functional safety concept	No. Assumptions made for internal development.	Yes
Allocation of end equipment requirements to sub-systems, hardware components, and software components	No. Assumptions made for internal development.	Yes
Definition of hardware component safety requirements	Yes	No
Hardware component architecture and design execution	Yes	No
Hardware component functional safety analysis	Yes	No
Hardware component verification and validation (V&V)	V&V executed to support internal development.	Yes
Integration of hardware component into end equipment	No	Yes
Verification of IC performance in end equipment	No	Yes

Table B-1. Activities Performed by Texas Instruments versus Performed by the customer (continued)

Functional Safety Lifecycle Activity[1]	TI Execution	Customer Execution
Selection of safety mechanisms to be applied to IC	No	Yes
End equipment level verification and validation	No	Yes
End equipment level functional safety analysis	No	Yes
End equipment level functional safety assessment	No	Yes
End equipment release to production	No	Yes
Management of functional safety issues in production	Support provided as needed	Yes

(1) For component technical questions, ask our TI E2E™ support experts.

B.3 Information Provided

Texas instruments has summarized what it considers the most critical functional safety work products that are available to the customer either publicly or under a nondisclosure agreement (NDA). NDAs are required to protect proprietary and sensitive information disclosed in certain functional safety documents.

Table B-2. Product Functional Safety Documentation

Deliverable Name	Contents
Functional Safety Manual	User guide for the functional safety features of the product, including system level assumptions of use.
Functional Safety Analysis Report	Results of all available functional safety analysis documented in a format that allows computation of custom metrics.

C Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

DATE	REVISION	NOTES
February 2024	*	Initial Release

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265