Application Note

Functionally Safe Automotive Xilinx ZynQ UltraScale+ MPSoC Using Dialog PMICs

AN-PM-104

Abstract

This application note presents a Dialog Semiconductor proposal to meet the functional safety requirements of a system based on a Xilinx ZynQ® UltraScale+™ MPSoC.

The application note presents the power and functional safety requirements and describes the features and functionality that the Dialog solution has included to meet these requirements.

Contents

Figures

Tables

1 Terms and Definitions

AEC-Q100	Automotive Electronics Council (http://www.aecouncil.com/) failure mechanism based stress test qualification
ASIL-C	Automotive safety integrity level, level C
FIT	Failures in time
FPD	Full power domain
FuSa	Functional safety
LPD	Low power domain
PL	Programmable logic
PS	Processing system
SoC	System on a chip
ZU	ZynQ Ultrascale

2 References

[1] DA9062-A, Datasheet, https://www.dialog-semiconductor.com/products/da9062-a

[2] DA9063L-A, Datasheet, https://www.dialog-semiconductor.com/products/da9063l-a

[3] DA9213-A, Datasheet, https://www.dialog-semiconductor.com/products/da9213-A

[4] GreenPAK Designer Software & User Guide, Dialog Semiconductor

[5] SLG46620 Voltage Monitoring GreenPAK Design File for FuSa, Dialog Semiconductor (must download GreenPAK Designer Software to open)

[6] SLG46620G, Datasheet, https://www.dialog-semiconductor.com/products/slg46620

Note: AECQ Grade 2 version coming early 2019 (SLG46620-AG)

3 Introduction

The following are examples of the requirements for meeting a functional safety criteria:

- AEC-Q100 grade 2 or higher
- ASIL-B or higher
- Window watchdog timer
- Programmable power sequencer controller
- GPIOs in order to control external components
- Satellite external power device to scale and support safety shutdown
- Companion external power monitor device
- Safety critical blocks should be powered independently from non-safety critical blocks

Using the features available on Dialog devices, solutions are presented to meet the power and functional safety requirements for two Xilinx ZynQ SoC platforms.

4 Xilinx Platform Information

The power requirements for the two particular end applications are summarized in Table 1 and Table 2 below. Application #1 is a camera based application and application #2 is a central computer application. In this particular case both applications specified the PS block as having a safety critical requirement.

4.1 Application #1 (local)

Table 1: Xilinx Application #1 Power Requirements

Rail	V_{OUT}	I_{OUT}	Safety Critical Requirement
VCCINT	0.72 or 0.85 V	2 to 4 A	no (PL)
VAUX	1.8 V	0.5 A	no (PL)
VIO_3.3V	3.3 V	0.1 A	no (PL)
VCCPSINT	0.85 V	2 to 3 A	yes (PS)
VPSAUX	1.8 V	0.3 A	yes (PS)
VPS_MGTRAVCC	0.9 V	0.3 A	yes (PS)
VPS_MGTRAVTT	1.8 V	0.06 A	yes (PS)
VCCPSPLL	1.2 V	0.05 A	yes (PS)
VCC_PSIO	3.3 V	0.1 A	yes (PS)
VCCO_PSDDR	1.1 V	1 to 2 A	yes (PS)
VREF	1.25 V	0.001 A	yes (PS)
VIC1	5 V	0.1 A	yes (PS)
VIC3	1.3 V	End user defined	yes (PS)

4.2 Application #2 (central)

Table 2: Xilinx Application #2 Power Requirements

Rail	V_{OUT}	I_{OUT}	Safety Critical Requirement
VCCINT	0.85 V	12 to 20 A	no (PL)
VAUX	1.8 V	1 to 2 A	no (PL)
VPLDDR	1.2 or 1.5 V	3 to 6 A	no (PL)
VMGTRAVCC	0.9 V	0.6 A	no (PL)
VMGTRAVAUX	1.8 V	0.1 A	no (PL)
VMGTAVTT	1.2 V	1 A	no (PL)
VIO_3.3V	3.3 V	0.1 A	no (PL)
VCCPSINT	0.85 V	2 to 3 A	yes (PS)
VPSAUX	1.8 V	0.3 A	yes (PS)
VPS_MGTRAVCC	0.85 V	0.3 A	yes (PS)
VCC_PSPLL	1.2 V	0.05 A	yes (PS)
VCC_PSIO	3.3 V	0.5 A	yes (PS)
VCCO_PSDDR	1.1 or 1.2 V	1 to 2 A	yes (PS)
VPSA_MGTRAVTT	1.8 V	0.1 A	yes (PS)
VREF	1.25 V	0.001 A	yes (PS)

5 Dialog Solution

The Dialog solution for each application consists of distributed power comprising of one or more system PMICs and sub-PMICs and GreenPAK Configurable Mixed-signal ICs (CMICs), implemented as customized external voltage monitoring devices.

System PMICs provide power and the intelligent power management control for the solution with the sub-PMICs providing the high current requirements. The GreenPAK can be programmed to perform many functions to address the varied safety requirement of different automotive systems. In this proposal, the GreenPAK is implemented as an external voltage monitor to provide an added layer of reliability to the overall solution.

5.1 ASIL-C Functional Safety Compliance

5.1.1 AEC-Q100 Grade 2 or Higher

All Dialog PMICs and sub-PMICs in the proposal are qualified to AEC-Q100 grade 2. The GreenPAK CMIC is undergoing AEC-Q100 grade 2 qualification with completion scheduled for early 2019.

5.1.2 ASIL-B or Higher

The Dialog power management chipset has various monitoring functions incorporated. These can be augmented by external voltage monitoring implemented through a GreenPAK CMIC to create a FuSa compliant system.

On-chip voltage monitoring is available on DA9063L-A. The voltage monitoring is configured to automatically monitor all regulator outputs of the DA9063L-A for over or under output voltage errors.

Additionally, three external ADC channel inputs are available to the DA9063L-A. These are used to monitor external regulator outputs and also generate an error condition if any of those outputs deviate outside of a programmable upper or lower threshold range.

DA9062-A has a reliability of 9 FIT. DA9063L-A has a reliability of 5 FIT and DA9213-A a reliability of 2 FIT.

Redundant voltage monitoring functions can be implemented in a GreenPAK CMIC. The chip design can be easily customized to accommodate the specific needs of the system. The SLG46620-AG GreenPAK CMIC can be configured to monitor under and over voltage errors with programmable threshold ranges, generate fault flags or customized corrective actions, and integrate additional functions such as watchdog timer, reset, power down, etc.

Note: The aforementioned FIT rates do not consider the inbuilt safety mechanisms and are actually lower than indicated. An FMEDA on the overall application will be required in order to determine their actual value and the final level of ASIL compliance.

5.1.3 Window Watchdog Timer with Question/Answer Function

Both DA9062-A and DA9063L-A provide a watchdog timer with programmable timeout. Timeout can be set between 2 seconds and 128 seconds. The internal watchdog is 'kicked' by the SoC via either an I^2C write to the watchdog bit within the device or toggling the KEEP_ACT hardware pin via a GPO pin on the SoC.

The SoC I^2C write or hardware pin toggle must occur prior to the selected timeout, but spaced apart more than a specified duration. If the SoC performs the kick too quickly or slowly the watchdog generates an error and causes the PMIC to shut down.

5.1.4 Programmable Power Sequencer Controller

Both DA9062-A and DA9063L-A include a programmable power sequencer controller. All internal regulators can be added to the sequencer to control the start-up and shutdown sequencing.

5.1.5 GPIOs to Control External Components

Both DA9062-A and DA9063L-A can include changes to GPIO levels in the sequencer. In this way external regulators (such as the DA9214-A sub-PMIC) can be added to the sequence controlled regime. If the system PMIC detects a fault condition that triggers a shutdown/reset the sub-PMIC is also powered off as part of the shutdown sequence.

5.1.6 Satellite External Power Device to Scale and Support Safety Shutdown

DA9213-A is a sub-PMIC providing a high current supply for PL domain power requirements. It includes automatic thermal and over-current protection.

5.1.7 Companion External Power Monitor Device

In these proposals, the SLG46220-AG GreenPAK provides redundant under and over voltage monitoring as well as fault signal monitoring. If the IC detects any fault conditions, it triggers a reset signal.

The References section of this document contains a link to download the GreenPAK Designer Software as well as the GreenPAK voltage monitoring design file. The design file can be downloaded to quickly program the SLG46620-AG to function as the voltage monitoring IC described in this proposal. The design file can also be easily modified using the schematic capture based GreenPAK Designer Software tool to create a custom voltage monitoring IC that accommodates the unique safety requirements of a system.

5.1.8 External Error Indication

nRESET is a signal from the DA9062-A or DA9063L-A that is used to hold the system in a reset state. The logic-low signal nRESET is de-asserted when the supply rail start-up sequence has finished. It is asserted before the shutdown sequence begins.

Events that trigger nRESET to be asserted are:

- Start-up sequencer in operation
- The SoC issues a shutdown command via I^2C or hardware control pin
- Device over-temperature detection
- Watchdog timer timeout
- A monitored regulator exceeding the output voltage tolerance threshold (over or under)
- A brownout is detected on the input supply

The signal nRESET can be configured to be push-pull or open drain. An external pull-up resistor is required for the open-drain configuration. This allows multiple reset signals to pull the signal low (ORed together).

FAULT_IND is an additional signal that provides a fault signal to the system. The signal persists through a reset of the system, only being cleared by a complete power down of the system.

5.2 Functional Safety Compliance States

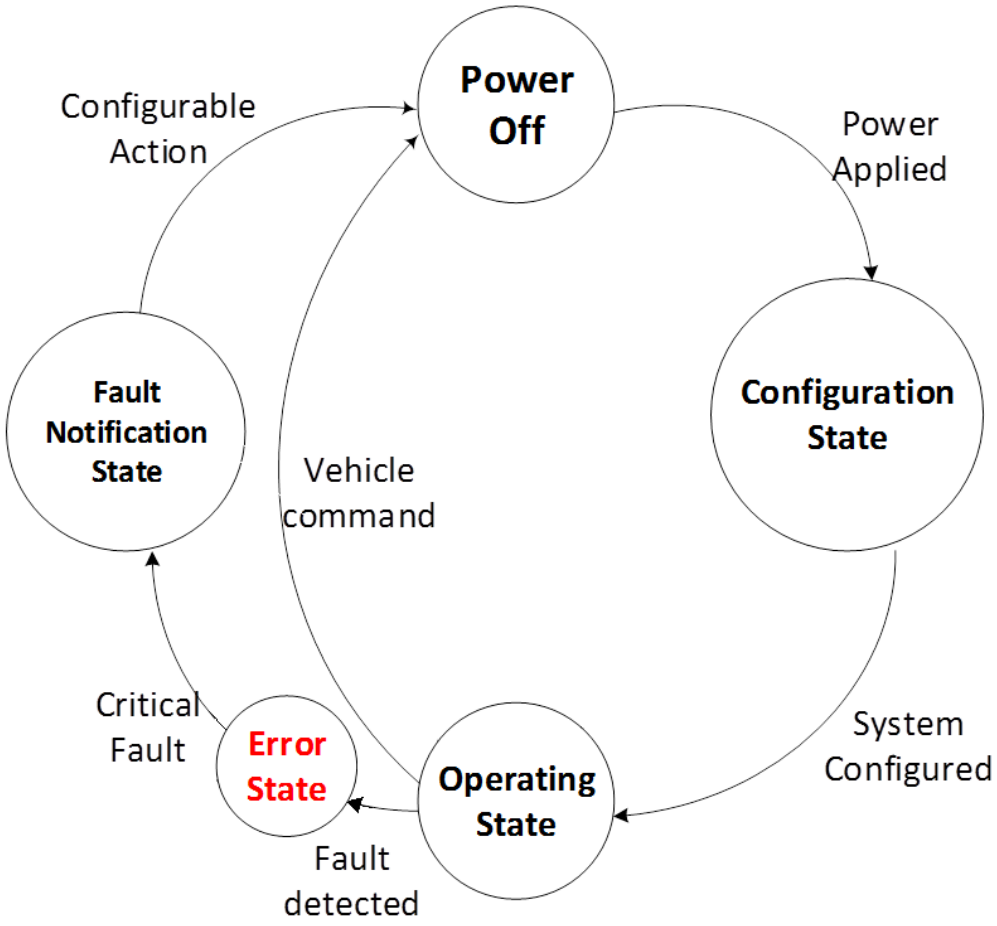

Figure 1: Element Operating States

Table 3: Operating States

State	Safety Function Available	Safe State	Primary Data Input	Primary Data Output	Power Domains	ZU + LPD	ZU + FPD	ZU + PL
Power off	NO	YES	Don't care	Don't care	OFF	OFF	OFF	OFF
Configuration	NO	NO	Configured	Configured	ON	ON	ON	ON
Operating	YES	YES	Functional	Functional	ON	ON	ON	ON
Error	NO	YES	Configured	Configured	ON	ON	ON	ON
Fault notification	NO	YES	Don't care	Don't care	OFF	OFF	OFF	OFF

5.3 Application #1 Proposal

Figure 2 shows a solution for the Xilinx application #1 platform.

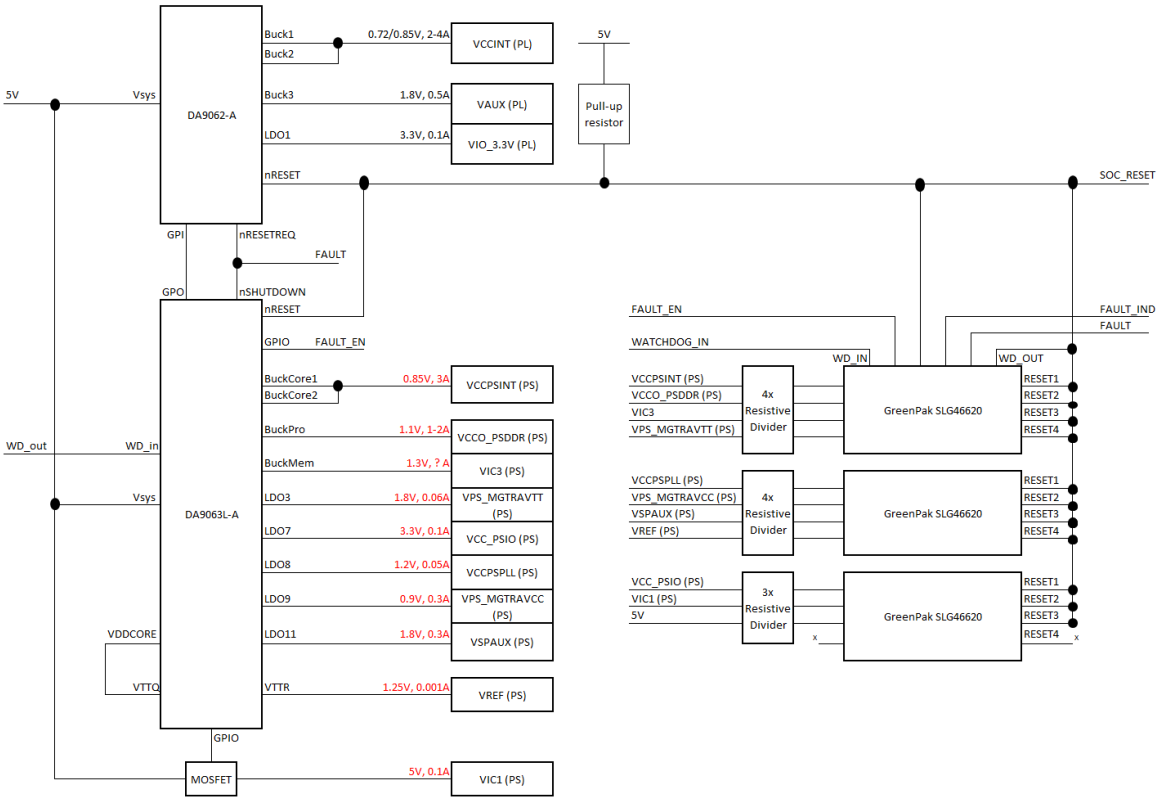

Figure 2: Application #1 Solution using GreenPAK™ External Voltage Monitoring

5.4 Application #2 Proposal

Figure 3 shows a solution for the Xilinx application #2 platform.

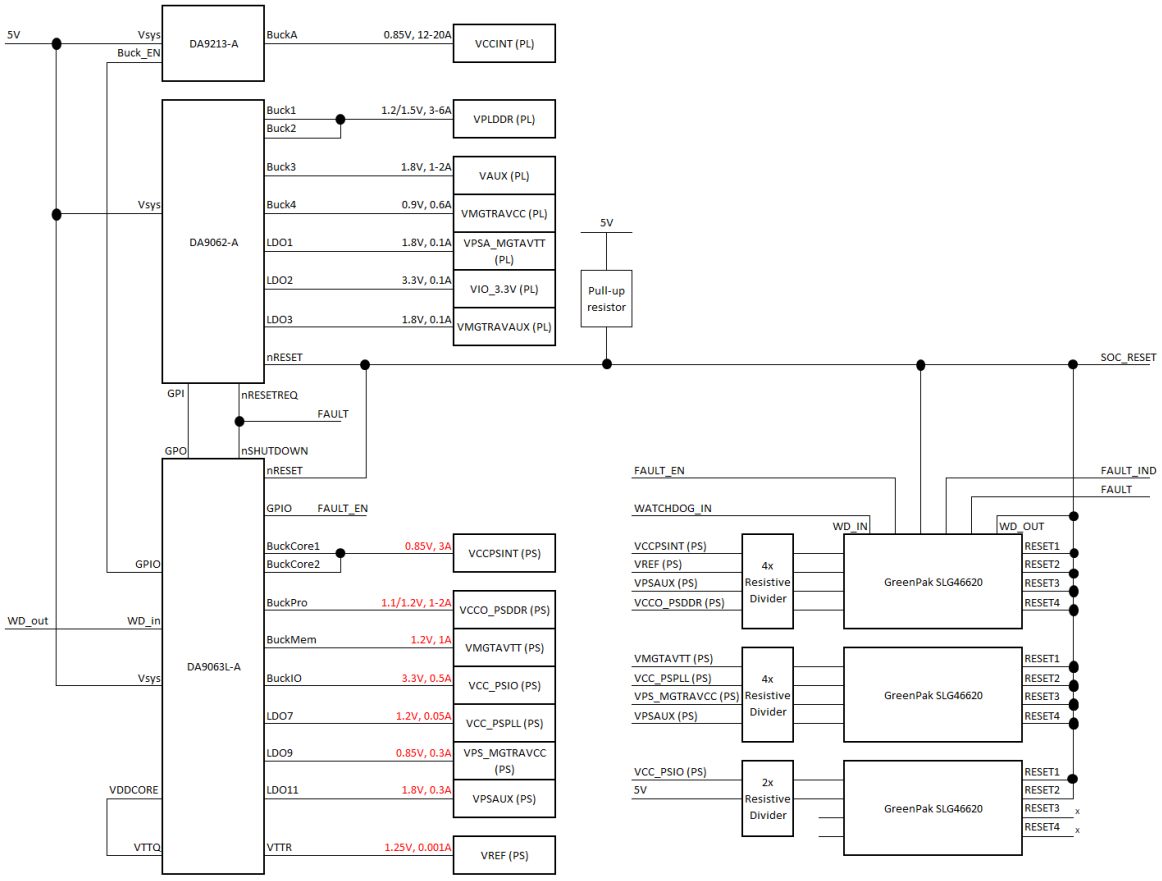

Figure 3: Application #2 Solution using GreenPAK™ External Voltage Monitoring

5.5 Theory of Operation

In application #1 and #2, signal SOC_RESET is held low by the ORed combination of DA9062-A nRESET, DA9063L-A nRESET, and the ORed RESET outputs from the Dialog voltage monitoring devices.

After DA9062-A and DA9063L-A have completed their respective start-up sequences they each release their nRESET signals. If a monitored output rail is within its required output voltage range the respective RESET signal on the voltage monitoring device is also released.

At the end of the DA9063L-A start-up sequence the GPIO output control FAULT_EN is set high.

Once all start-up sequences are completed and all monitored output voltage rails are within their specified voltage range SOC_RESET is released allowing the SoC to begin operation.

If an out of range voltage event occurs or the watchdog timeout is triggered a falling edge is generated on SOC_RESET.

The falling edge resets the SoC and clocks the D-latch which latches the state of FAULT_EN. This provides a fault indication to the system on the Q output of the D-latch. The D-latch nQ output also drives DA9062-A nRESETREQ and DA9063L-A nSHUTDOWN to a logic low, triggering a shutdown of both PMICs and in the case of application #2 also shutting down the sub-PMIC.

6 Conclusion

Using the features and flexibility available on Dialog devices it is possible to meet the power and functional safety requirements of Xilinx ZU+ platforms.

Revision History

Revision	Date	Description
0.1 - DRAFT	21-Dec-2017	Initial version
0.2 - DRAFT	28-Dec-2017	Edit following review
1.0	26-Apr-2018	Added Silego voltage monitoring, state diagrams and theory of operation.
1.1	04-Jan-2019	Typo corrections and added FMEDA note to 5.1.2

Functionally Safe Automotive Xilinx ZynQ UltraScale+ MPSoC

Status Definitions

Status	Definition
DRAFT	The content of this document is under review and subject to formal approval, which may result in modifications or additions.
APPROVED or unmarked	The content of this document has been approved for publication.

Disclaimer

Contacting Dialog Semiconductor

United Kingdom (Headquarters)
Dialog Semiconductor (UK) LTD
Phone: +44 1793 757700

Germany
Dialog Semiconductor GmbH
Phone: +49 7021 805-0

The Netherlands
Dialog Semiconductor B.V.
Phone: +31 73 640 8822

Email:

North America
Dialog Semiconductor Inc.
Phone: +1 408 845 8500

Japan
Dialog Semiconductor K. K.
Phone: +81 3 5769 5100

Taiwan
Dialog Semiconductor Taiwan
Phone: +886 281 786 222

Web site:

Hong Kong
Dialog Semiconductor Hong Kong
Phone: +852 2607 4271

Korea
Dialog Semiconductor Korea
Phone: +82 2 3469 8200

China (Shenzhen)
Dialog Semiconductor China
Phone: +86 755 2981 3669

China (Shanghai)
Dialog Semiconductor China
Phone: +86 21 5424 9058

enquiry@diasemi.com www.dialog-semiconductor.com

