

Application Note

Tamper Detector

AN-CM-313

Abstract

This application note describes a tamper detector design using the SLG46811 IC as an emulated SPI master to drive Dialog's AT45DB161E Flash memory

Tamper Detector

Contents

Abstract	1
Contents	2
Figures	2
Tables	3
1 Terms and Definitions	4
2 References	4
3 Introduction	5
4 Principle	5
5 Internal Blocks Configuration	7
5.1 MS ACMP Configuration	7
5.2 Oscillator Configuration.....	8
5.3 EPG Configuration and Data	8
5.4 LUTs Configurations	10
5.5 DFFs Configurations	11
5.6 Filter / Edge Detector Configuration.....	12
5.7 CNT/DLY0 Configuration	12
5.8 P DLY Configuration	12
5.9 IO Pins Configurations	13
5.10 I ² C Macrocell Configuration	13
6 Design Verification Using Hardware Prototype	13
7 Conclusions	14
8 Further Considerations	14
Revision History	15

Figures

Figure 1: Tamper Detector Basic Structure.....	5
Figure 2: Timing Diagram of Tamper Detector.....	6
Figure 3: Internal Design of tamper detector based on SLG46811 in GreenPAK Designer Software..	7
Figure 4: MS ACMP Configuration	7
Figure 5: Oscillator1 Configuration.....	8
Figure 6: EPG Configuration	8
Figure 7: EPG Waveform	9
Figure 8: LUTs Configurations.....	10
Figure 9: DFFs Configurations	11
Figure 10: Filter / Edge Detector Configuration.....	12
Figure 11: CNT/DLY0 (MF0) Configuration.....	12
Figure 12: P DLY Configuration	12
Figure 13: IO Pins Configurations	13
Figure 14: EPG OUT0. Data = 5Ah to be stored in Flash memory.....	13
Figure 15: Zoomed EPG OUT0.....	14
Figure 16: EPG OUT1. Data = A5h to be stored in Flash	14

Tamper Detector

Tables

Table 1: MOSI (SLG46811 as a master, Flash memory as a slave) 6

Tamper Detector

Terms and Definitions

DFF	D flip flop
DI w/o ST	Digital input without Schmidt trigger
EPG	Extended pattern generator
IC	Integrated Circuit
I2C	Inter-integrated circuit (bus)
MS ACMP	Multichannel Sampling Analog Comparator
OE	Output Enable
SHR	Shift register
SPI	Serial peripheral interface

1 References

- [1] [SLG46811, Datasheet, Dialog Semiconductor](#)
- [2] <https://en.wikipedia.org/wiki/DataFlash>

Tamper Detector

2 Introduction

Tamper detection is a function widely used within critical infrastructure systems such as power meters, water meters, security and fire panels, and any other products where a trigger input needs to be detected and the event recorded in non-volatile memory (Flash memory). The SLG46811 GreenPAK mixed-signal IC is ideally suited for this tamper-detection role when paired with the AT45DB161E Flash memory for recording the event.

3 Principle

Figure 1 shows the basic design of the tamper detector. The devices with low pin-count serial Data Flash® interface [2] are the easiest to set up for a tamper detector as we can use the page erase and page write as one instruction while bypassing the Write Enable signal of the Flash before said command => one command Byte, 3 address Bytes and data Bytes (Figure 2 and Table 1). 0x82 is the command to program Main Memory Page through Buffer 1 with Built-In Erase.

CS, MOSI, and CLK pins are configured as Push Pull. Trigger sources that force SLG46811 to write data to flash memory are:

- external signal from GPIO;
- ACMP with low Vdd level detection. When $V_{dd} < 3V$, Trigger #1 occurs.

SLG46811 can operate with flash memory if enable EN input is HIGH.

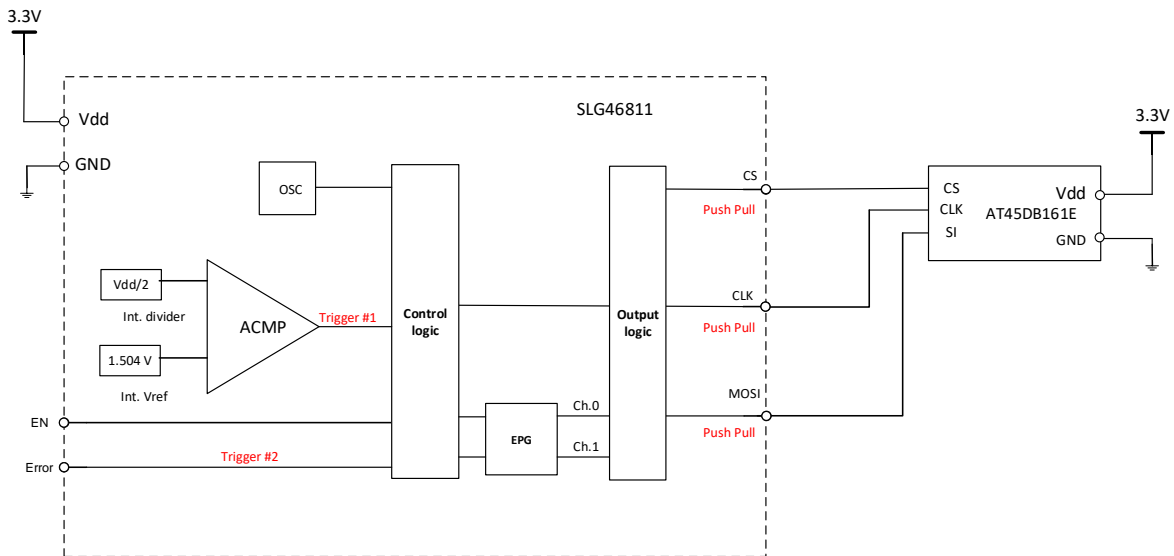


Figure 1: Tamper Detector Basic Structure

Tamper Detector

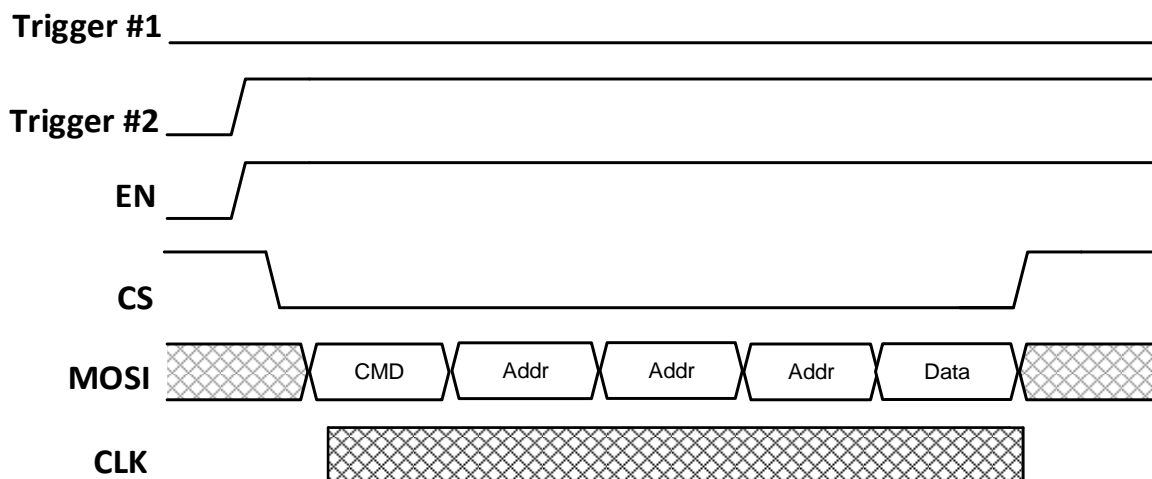


Figure 2: Timing Diagram of Tamper Detector

Table 1: MOSI (SLG46811 as a master, Flash memory as a slave)

EPG OUTX	CMD	Addr	Addr	Addr	Data
EPG OUT0	0x82	F1	00	00	5A
EPG OUT1	0x82	F1	40	00	A5

The SLG46811 design (Figure 3) sets up the Extended Pattern Generator as a SPI master to generate the command sequence and the specific data for the trigger. While the signal at PIN10 (Trigger #2) goes HIGH and the signal at PIN2 (EN) is HIGH, a LOW-level signal is generated at PIN5 (CS). While CS is LOW the CLK signal is generated at PIN11 (CLK) to clock the command sequence out at PIN12 (MOSI).

DFF9 and DFF5 are used to generate a pulse passing through 4-bit LUT0 and 2-bit LUT2 to trigger one-shot (CNT0). A LOW level of the one-shot generates the CS signal (PIN5). Similarly, the Under-Voltage sequence is generated at MOSI when Vdd drops below the MS ACMP voltage reference.

When Vdd drops below the comparator voltage reference, DFF12 and DFF8 generate a pulse to the 4-bit LUT0, just as with Trigger #2.

DFF3 serves as a frequency divide by 2. DFF2 serves as CLK at PIN11 delayed by 1 clock pulse after CS signal. After data transition the PDLY and 2-bit LUT0 are used to set DFF2 (to 0), and 2-bit LUT1 used to reset DFF3 (to initial value) and EPG (to initial value).

3-bit LUT4, 3-bit LUT9 and 3-bit LUT12 are used for muxing EPG outputs according to trigger conditions.

EPG is used to store pre-programmed data. EPG OUT0 generates data while Vdd voltage goes below threshold, and OUT1 generates data relative to the input pulse (at PIN10).

EPG can retain up to 92 bits of pre-programmed data for each output. To change the transaction data size it is necessary to set the CNT0 data (but CNT0 data cannot be more than 92).

Tamper Detector

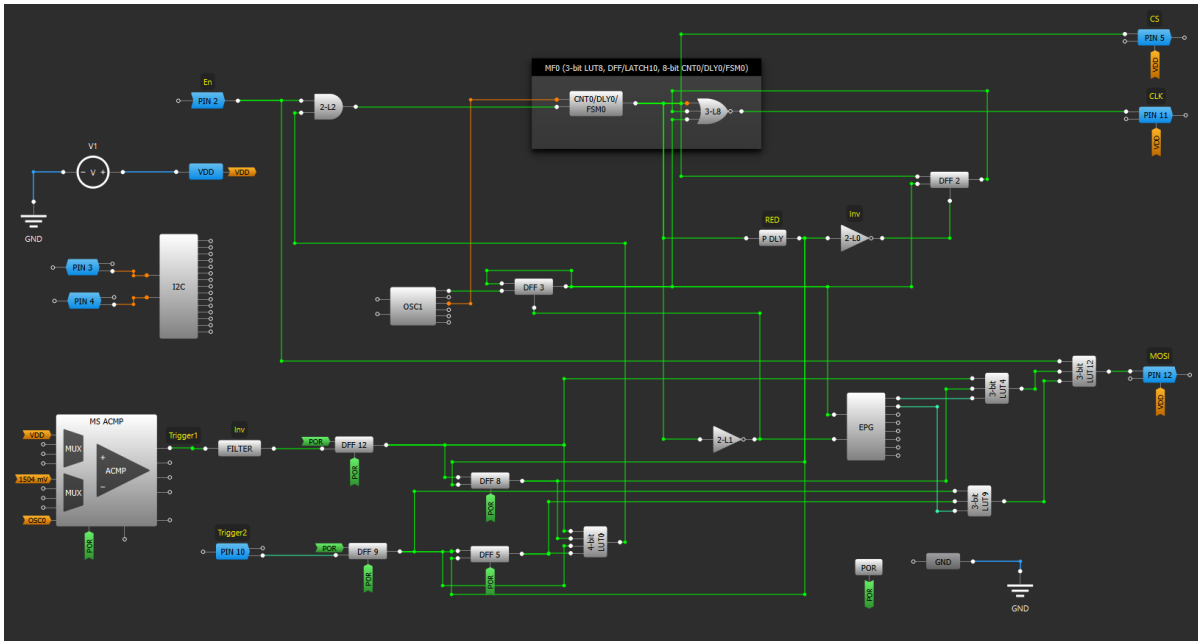


Figure 3: Internal Design of tamper detector based on SLG46811 in GreenPAK Designer Software

4 Internal Blocks Configuration

4.1 MS ACMP Configuration

MS ACMP	
ACMP mode:	Regular ACMP
Number of channels:	1
Enable mode:	High Level Activatic
Output result appearance:	One by one
Sampling clock:	OSCO
VDD input:	Enable
Temp Sensor input:	Disable
Force bandgap on:	Enable
Channel 0	
Ch0 output nReset:	Disable
Hysteresis:	Disable
IN+ gain:	x0.5
IN+ source:	VDD
IN- source:	1504 mV

Figure 4: MS ACMP Configuration

Tamper Detector

4.2 Oscillator Configuration

OSC1	
Control pin mode:	Power down
Power down input:	Disable
OSC power mode:	Auto Power On
Clock selector:	OSC
'OSC1' frequency:	25 MHz
'CLK' predivider by:	24
'OUT' second divider by:	2
Start with delay:	Enable

Figure 5: Oscillator1 Configuration

4.3 EPG Configuration and Data

Properties EPG	
CNT overflow/keep:	Stop at boundary
Initial data:	0
Data:	Edit waveforms
Output 0:	EPG OUT0
Output 1:	EPG OUT1
Output 2:	EPG OUT2
Output 3:	EPG OUT3
Output 4:	EPG OUT4
Output 5:	EPG OUT5
Output 6:	EPG OUT6
Output 7:	EPG OUT7

Figure 6: EPG Configuration

Tamper Detector



Figure 7: EPG Waveform

Tamper Detector

4.4 LUTs Configurations

2-bit LUT2/PGEN

Type: LUT

IN3	IN2	IN1	IN0	OUT
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Standard gates: All to 0 All to 1 Invert

Defined by user: AND Regular shape

4-bit LUT0/DFE/LATCH16

Type: LUT

IN3	IN2	IN1	IN0	OUT
0	0	0	0	0
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	0
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	0
1	1	0	1	0
1	1	1	0	1
1	1	1	1	0

Standard gates: All to 0 All to 1 Invert

Defined by user: Defined by user Regular shape

3-bit LUT8 (MF0)

IN3	IN2	IN1	IN0	OUT
0	0	0	0	1
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Standard gates: All to 0 All to 1 Invert

Defined by user: NOR Regular shape

3-bit LUT4/DFE/LATCH6/Shift Regis...

Type: LUT

IN3	IN2	IN1	IN0	OUT
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Standard gates: All to 0 All to 1 Invert

Defined by user: Defined by user Regular shape

3-bit LUT9 (MF1)

Multi-function mode: LUT

IN3	IN2	IN1	IN0	OUT
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Standard gates: All to 0 All to 1 Invert

Defined by user: Defined by user Regular shape

3-bit LUT12 (MF4)

Multi-function mode: LUT

IN3	IN2	IN1	IN0	OUT
0	0	0	0	1
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Standard gates: All to 0 All to 1 Invert

Defined by user: Defined by user Regular shape

Figure 8: LUTs Configurations

Tamper Detector

4.5 DFFs Configurations

DFF/LATCH12 (MF2)

Multi-function mode: DFF/LATCH

Mode: DFF

nSET/nRESET option: nRESET

Initial polarity: Low

Q output polarity: Non-inverted (Q)

Information

Normal operation

D	CLK	Q(t)	nQ(t)
0	↑	0	1
0	↓	t - 1	t - 1
1	↑	1	0
1	↓	t - 1	t - 1

t - 1 - previous state;
 nRESET = 0 => Q = 0; nQ = 1;
 nRESET = 1 => normal operation;
 nSET = 0 => Q = 1; nQ = 0;
 nSET = 1 => normal operation;

3-bit LUT7/DFF/LATCH9/Shift Regis...

Type: DFF / LATCH

Mode: DFF

nSET/nRESET option: nRESET

Initial polarity: Low

Q output polarity: Non-inverted (Q)

Active level for RST/SET: Low level

Information

Normal operation

D	CLK	Q(t)	nQ(t)
0	↑	0	1
0	↓	t - 1	t - 1
1	↑	1	0
1	↓	t - 1	t - 1

t - 1 - previous state;
 nRESET = 0 => Q = 0; nQ = 1;
 nRESET = 1 => normal operation;
 nSET = 0 => Q = 1; nQ = 0;
 nSET = 1 => normal operation;

3-bit LUT6/DFF/LATCH8/Shift Regis...

Type: DFF / LATCH

Mode: DFF

nSET/nRESET option: nRESET

Initial polarity: Low

Q output polarity: Non-inverted (Q)

Active level for RST/SET: Low level

Information

Normal operation

D	CLK	Q(t)	nQ(t)
0	↑	0	1
0	↓	t - 1	t - 1
1	↑	1	0
1	↓	t - 1	t - 1

t - 1 - previous state;
 nRESET = 0 => Q = 0; nQ = 1;
 nRESET = 1 => normal operation;
 nSET = 0 => Q = 1; nQ = 0;
 nSET = 1 => normal operation;

3-bit LUT3/DFF/LATCH5

Type: DFF / LATCH

Mode: DFF

Second Q select: None

nSET/nRESET option: nRESET

Initial polarity: Low

Q output polarity: Non-inverted (Q)

Active level for RST/SET: Low level

Information

Normal operation

D	CLK	Q(t)	nQ(t)
0	↑	0	1
0	↓	t - 1	t - 1
1	↑	1	0
1	↓	t - 1	t - 1

t - 1 - previous state;
 nRESET = 0 => Q = 0; nQ = 1;
 nRESET = 1 => normal operation;
 nSET = 0 => Q = 1; nQ = 0;
 nSET = 1 => normal operation;

3-bit LUT0/DFF/LATCH2

Type: DFF / LATCH

Mode: DFF

Second Q select: Q of first DFF

nSET/nRESET option: nSET

Initial polarity: High

Q output polarity: Non-inverted (Q)

Active level for RST/SET: Low level

Information

Normal operation

D	CLK	Q(t)	nQ(t)
0	↑	0	1
0	↓	t - 1	t - 1
1	↑	1	0
1	↓	t - 1	t - 1

t - 1 - previous state;
 nRESET = 0 => Q = 0; nQ = 1;
 nRESET = 1 => normal operation;
 nSET = 0 => Q = 1; nQ = 0;
 nSET = 1 => normal operation;

3-bit LUT1/DFF/LATCH3

Type: DFF / LATCH

Mode: DFF

Second Q select: None

nSET/nRESET option: nRESET

Initial polarity: Low

Q output polarity: Inverted (nQ)

Active level for RST/SET: Low level

Information

Normal operation

D	CLK	Q(t)	nQ(t)
0	↑	0	1
0	↓	t - 1	t - 1
1	↑	1	0
1	↓	t - 1	t - 1

t - 1 - previous state;
 nRESET = 0 => Q = 0; nQ = 1;
 nRESET = 1 => normal operation;
 nSET = 0 => Q = 1; nQ = 0;
 nSET = 1 => normal operation;

Figure 9: DFFs Configurations

4.6 Filter / Edge Detector Configuration

FILTER/EDGE DET

Type:

Output polarity:

Information

Delay and Filtered Pulse Width (Typical)

VDD (V)	Delay (ns)	Pulse Width (ns)
-	-	-
-	-	-
-	-	-

Figure 10: Filter / Edge Detector Configuration

4.7 CNT/DLY0 Configuration

8-bit CNT0/DLY0/FSM0 (MF0)

Mode:

Counter data:
(Range: 1 - 255)

Pulse width (typical): 157.44 us [Formula](#)

Edge select:

DLY IN init. value:

Output polarity:

Up signal sync.:

Mode signal sync.:

FSM SET/RST Selection:

Connections

Clock:

Clock source: OSC1 Freq. /24 /4

Clock frequency: 260.417 kHz

Figure 11: CNT/DLY0 (MF0) Configuration

4.8 P DLY Configuration

P DLY

Mode:

Delay value:

Information

Delay and pulse width

VDD (V)	Delay (ns)	Pulse width (ns)
-	-	-
-	-	-
-	-	-

Figure 12: P DLY Configuration

Tamper Detector

4.9 IO Pins Configurations

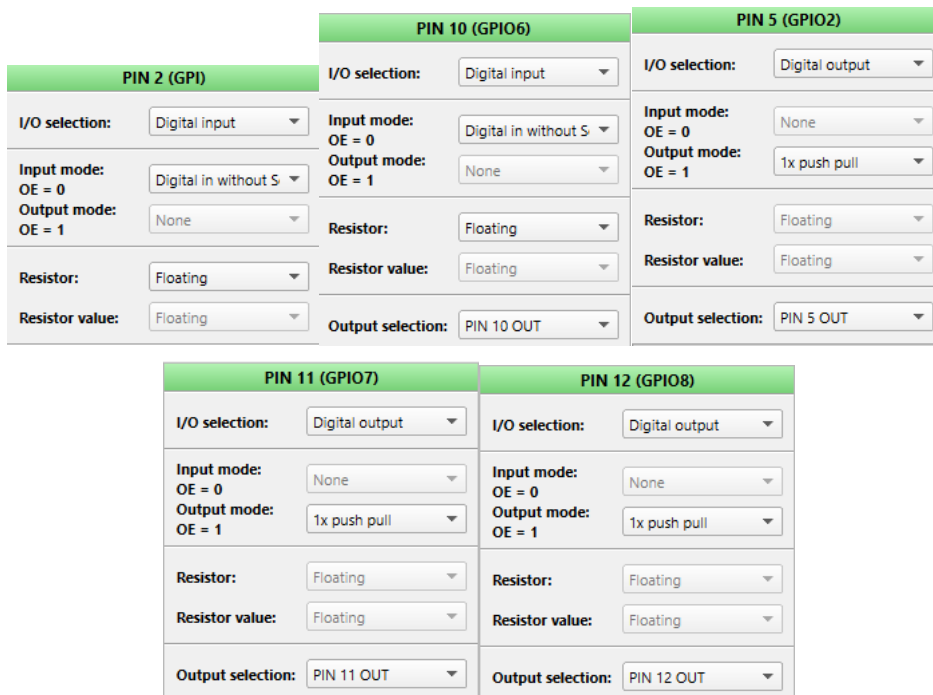


Figure 13: IO Pins Configurations

4.10 I²C Macrocell Configuration

I²C Macrocell uses default settings.

5 Design Verification Using Hardware Prototype

The design was tested in hardware (SLG46811 + AT45DB161 flash), and **Error! Reference source not found.** - Figure 16 show the waveforms sent to the flash memory while hardware prototyping.

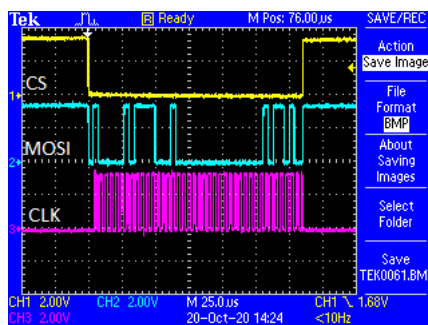


Figure 14: EPG OUT0. Data = 5Ah to be stored in Flash Memory

Tamper Detector

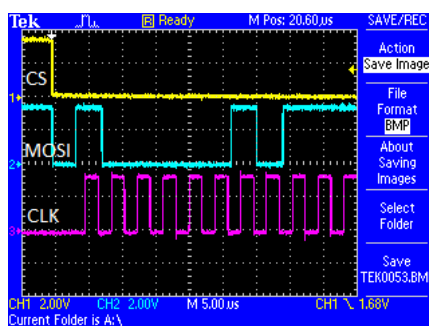


Figure 15: Zoomed EPG OUT0

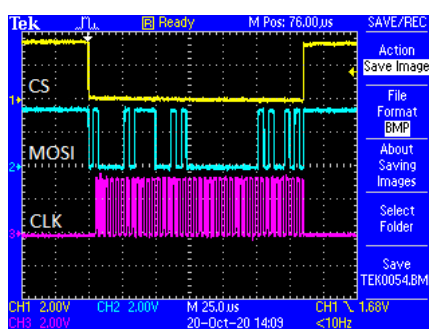


Figure 16: EPG OUT1. Data = A5h to be stored in Flash

7 Conclusions

Dialog SLG46811 is a great solution for the development of a simple SPI master to drive flash memory. As usual with the GreenPAK family of products, the tamper and fault detection implementation described in this application is just one of many ways to perform this implementation. Additional advantages of "GreenPAK + AT45DB161E memory implementation" are quick design time, high level of configurability, low power consumption, small board area, and low cost.

8 Further Considerations

This design could be further enhanced by driving the Output pins to the Flash memory as Tristate when the EN input is driven low. This would allow a host microcontroller to access the Flash to read the Last Trigger results and to use the Flash for general storage. The host micro would need to tristate its CLK, MOSI and /CS pins when it drives the EN pin is high.

Revision History

Revision	Date	Description
1.0	15-Mar-2021	Initial version.

Tamper Detector

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

Information in this document is believed to be accurate and reliable. However, Dialog Semiconductor does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information. Dialog Semiconductor furthermore takes no responsibility whatsoever for the content in this document if provided by any information source outside of Dialog Semiconductor.

Dialog Semiconductor reserves the right to change without notice the information published in this document, including without limitation the specification and the design of the related semiconductor products, software and applications.

Applications, software, and semiconductor products described in this document are for illustrative purposes only. Dialog Semiconductor makes no representation or warranty that such applications, software and semiconductor products will be suitable for the specified use without further testing or modification. Unless otherwise agreed in writing, such testing or modification is the sole responsibility of the customer and Dialog Semiconductor excludes all liability in this respect.

Customer notes that nothing in this document may be construed as a license for customer to use the Dialog Semiconductor products, software and applications referred to in this document. Such license must be separately sought by customer with Dialog Semiconductor.

All use of Dialog Semiconductor products, software and applications referred to in this document are subject to Dialog Semiconductor's [Standard Terms and Conditions of Sale](#), available on the company website (www.dialog-semiconductor.com) unless otherwise stated.

Dialog and the Dialog logo are trademarks of Dialog Semiconductor plc or its subsidiaries. All other product or service names are the property of their respective owners.

© 2021 Dialog Semiconductor. All rights reserved.

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:

enquiry@diasemi.com

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:

www.dialog-semiconductor.com

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