19-5894; Rev 0; 6/11

Secure Authentication Starter Kit

General Description

The secure authentication starter kit is a highly programmable hardware/software system for development, lab testing, and demonstration of embedded applications that use Maxim's SHA-1-based secure authentication products. The system supports multiple options for demonstrating and developing both host SHA-1 computation and associated host communication with Maxim's 1-Wire® and I^{2}C-based SHA-1 slave ICs. Multiple options are supported for host SHA-1 computation development including fixed function processing with the Maxim DS2460, microcontroller(µC)-based with a Microchip PIC18F4550, and a Maxim-developed SHA-1 Verilog implementation (DSSHA1) used in conjunction with a Xilinx Spartan®-3A XC3S400A FPGA. Development capabilities for the host interface to Maxim's SHA-1 slaves are similarly supported with multiple options including the Maxim DS2482-100 I^{2}C-to-1-Wire line driver, software generation of 1-Wire waveforms with the PIC18F4550, and a Verilog implementation (DS1WM) with the Xilinx FPGA. The EV kit can be used alone or controlled with a PC over RS-232 or USB interfaces. Microcontroller software can be installed and tested through an in-circuit debugger port. A JTAG port allows changing the FPGA programming through standard Xilinx development tools. With its expansion ports (40 pins for the microcontroller, 120 pins for the FPGA), the board can be the development platform for complex designs.

The free software/firmware is available by request at https://support.maxim-ic.com/1-Wire.

Features

- ♦ **Complete Development System for Applications Using Maxim SHA-1 Products**
- ♦ **Starter Kit Board Includes Maxim's DS2460, DS2482-100, DS28CN01, and DS28E01 Devices for Rapid Development**
- ♦ **Other and Future Maxim SHA-1 Authenticators Supported Through Expansion Ports**
- ♦ **Embedded Host Development Options Supported with PIC18F4550 µC and Xilinx XC3S400A FPGA**
- ♦ **PC Connectivity with RS-232 and USB 2.0**
- ♦ **JTAG Connector Mates to Xilinx Platform Cables Through a Single Ribbon Cable**
- ♦ **120-Pin Expansion Port for FPGA**
- ♦ **In-Circuit Debugger Port for PIC18F4550**
- ♦ **40-Pin Expansion Port for PIC18F4550 Periphery**
- ♦ **Extension Ports for I^{2}C and 1-Wire Bus**
- ♦ **Jumper Configurable for µC or FPGA as I^{2}C Master**
- ♦ **Jumper Configurable for µC, FPGA, DS2482-100, or External 1-Wire Bus Master**
- ♦ **Six General-Purpose Pushbuttons and Indicator LEDs**
- ♦ **LED Indicators for Power and FPGA Load Done**
- ♦ **Free Evaluation Software Available by NDA**

Ordering Information

PART	TYPE
DSAUTHSK#	Secure Authentication Starter Kit

#Denotes a RoHS-compliant device that may include lead(Pb) that is exempt under the RoHS requirements.

Evaluates: DS28E01/DS28CN01/DS2460

Secure Authentication Starter Kit

Component List

ITEM TYPE	DESIGNATOR	LABEL	LOCATION (SEE FIGURE 1)	DESCRIPTION
PCB	—	—	—	PCB: Secure Authentication Starter Kit#, REV A
POWER SUPPLY				
LED	D9	—	B7	Red LED LNJ208R8ARA
Connector	J14	—	A6	2.1mm barrel socket PJ-002A-SMT
Jumper	JP9	USB, JACK	A6/A7, B6/B7	3 pins
Pushbutton	SW8	RESET POWER	B5	Normally open 7914J-1-000E
Test Point	TP5	TIP	A7	Inner contact of J14 (positive)
	TP6	RING	A6	Outer contact of J14 (negative)
	TP7	5V	B7	Raw 5V power rail
	TP8	—	B6/C6	Filtered 3.3V power rail before R47
	TP9	—	B6	Filtered 3.3V power rail
	TP10	—	C6	Filtered 1.2V power rail before R49
	TP11	—	C6	Filtered 1.2V power rail
	TP14	GND	I1	Access to local ground
	TP15	GND	B7	
	TP16	GND	H7	
	TP17	GND	I4	
	TP18	GND	C2	
	TP19	GND	C7	
IC	U24, U25	—	B6, C6	Step-down DC-DC converter (10 TDFN-EP*) Maxim MAX1556AETB+
	U26	—	B5	Triple voltage monitor and sequencer (20 TQFN-EP*) Maxim MAX16028TP+
SYSTEM CLOCK				
IC	U21, U23		E2	Single Schmitt-trigger inverter 74VHC1G14DF
	U22		E2/F2	16MHz oscillator Fox Electronics FXO-HC536R-16
PIC MICRO				
LED	D1, D2	—	B1	Green LED LNJ308G8TRA
Connector	J1	—	A4/A5	Mini USB, female DX3R005HN2E700
	J2	—	A1, A2, A3	DB9 connector 5788797-1
	J3	—	B3/B4	5-pin header, ICD port 4-102972-0
	J4	—	D2–D5	2 x 20-pin header PEC20DAAN
Jumper	JP4	uP-OW	E6	2 pins

Component List (continued)

ITEM TYPE	DESIGNATOR	LABEL	LOCATION (SEE FIGURE 1)	DESCRIPTION
Pushbutton	SW1	RB4 MICRO	B1	Normally open 7914J-1-000E
	SW2	RB5 MICRO	B1/C1	
IC	U2	—	B2/B3	RS-232 drivers/receivers (16 TSSOP) Maxim MAX232ACUE+
	U5	—	C3	Microcontroller PIC18F4550T-I/PT
FPGA				
LED	D3, D4	—	E1	Green LED LNJ308G8TRA
	D5	—	D1	
	D6	—	C1	
	D7	—	F1	Blue LED LTST-C191TBKT
Connector	J5	—	E5/F5	2mm spaced pin header, 2 x 7 pins 87759-1450
	J6	BANK 3	I4–I7	0.1-mil spaced pin header, 2 x 20 pins PEC20DAAN
	J7	BANK 0	I1–I4	
	J8	BANK 1	F1–I1	
Jumper Block	JB1	—	G3	2 x 3 pins 9-146252-0-01
Jumper	JP1	—	F3/G3	3 pins
	JP6	FPGA	E6	2 pins
Pushbutton	SW3	BANK 0 FPGA	E1/F1	Normally open 7914J-1-000E
	SW4	BANK 1 FPGA	E1	
	SW5	BANK 2 FPGA	D1	
	SW6	BANK 3 FPGA	C1	
	SW7	RESET	F4	
IC	U10	—	G2/G3, H2/H3	Spartan-3A FPGA XC3S400A-4FTG256C
	U11	—	F4	Gate NC7SV08P5X
	U12	—	E4/F4	PROM for FPGA XCF04SVOG20C
	U17, U19	—	G5, D5/E5, D6/E6	Dual-level translator (8 TDFN-EP*) Maxim MAX3394EETA+T
PIC/FPGA BRIDGE				
Test Point	TP1	RA6	C2	Signal input pin of U3
IC	U1	—	D2	Three-state bus buffer/line driver 74VHC1G125DF
	U3	—	C2	
	U4, U9	—	E3	
	U6	—	E3/F3	Octal transparent latch 74LCX573DTG
	U7	—	E3/F3, E4/F4	Low-voltage CMOS octal transceiver MC74LCX245DTR2G

Secure Authentication Starter Kit

Component List (continued)

ITEM TYPE	DESIGNATOR	LABEL	LOCATION (SEE FIGURE 1)	DESCRIPTION
IC	U8	—	C2	Single Schmitt-trigger inverter 74VHC1G14DF
I^2C				
Connector	J9	—	G7/H7	I^2C expansion port
Jumper	JP2	—	G5	Select SCL source for I^2C slaves
	JP3	—	F5	Select SDA source for I^2C slaves
	JP8	2482	F6	Enable 1-Wire extra strong pullup from DS2482-100
Test Point	TP2	SCL	H7	SCL line of I^2C bus
	TP3	SDA	I7	SDA line of I^2C bus
IC	U13	—	F7	Single-channel 1-Wire master (8 SO) Maxim DS2482S-100+
	U14	—	F6	1Kbit I^2C/SMBus EEPROM with SHA-1 engine (8 µSOP) Maxim DS28CN01U-A00+
	U15	—	F6	SHA-1 coprocessor with EEPROM (8 SO) Maxim DS2460S+
	U16	—	F5/F6	12-bit I^2C voltage-output DAC (6 SOT23) Maxim MAX5812MEUT
1-Wire				
Connector	J10	VPUP	E5	1-Wire pullup resistor
	J11	—	D7/E7	RJ11 1-Wire port 5520250-3
	J12	—	F7/G7	1-Wire expansion port
	J13	—	F7	TO-92 1-Wire socket 801-93-036-10-012000
Jumper	JP5	—	E5/F5, E6/F6	2 x 3 pins 9-146252-0-03
	JP7	—	E7	2 pins
	JP10	—	C5	3 pins
	JP11	—	C5	3 pins
Test Point	TP4	OW	D7	Data line of 1-Wire bus
	TP12	VPUP	D6	1-Wire V_{PUP} before R52
	TP13	VPUP	D7	1-Wire V_{PUP}
IC	U18	—	D6	ESD protection diode with resistors (6 TSOC) Maxim DS9503P+
	U20	—	E7	1Kb protected 1-Wire EEPROM with SHA-1 engine (6 TSOC) Maxim DS28E01P-100+

+Denotes a lead(Pb)-free/RoHS-compliant package.
**EP = Exposed pad.*

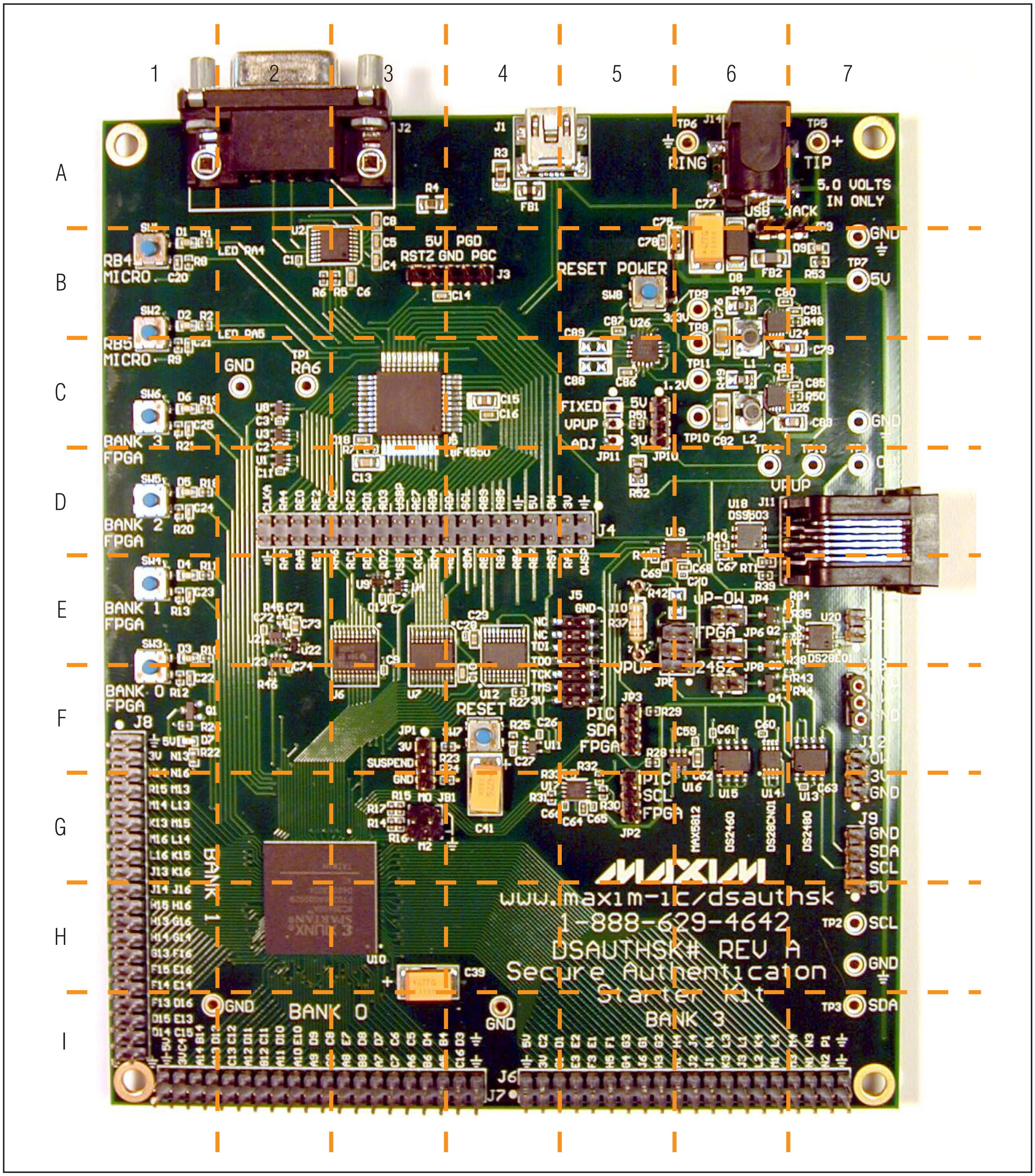

Figure 1. Secure Authentication Starter Kit Circuit Board with Reference Grid

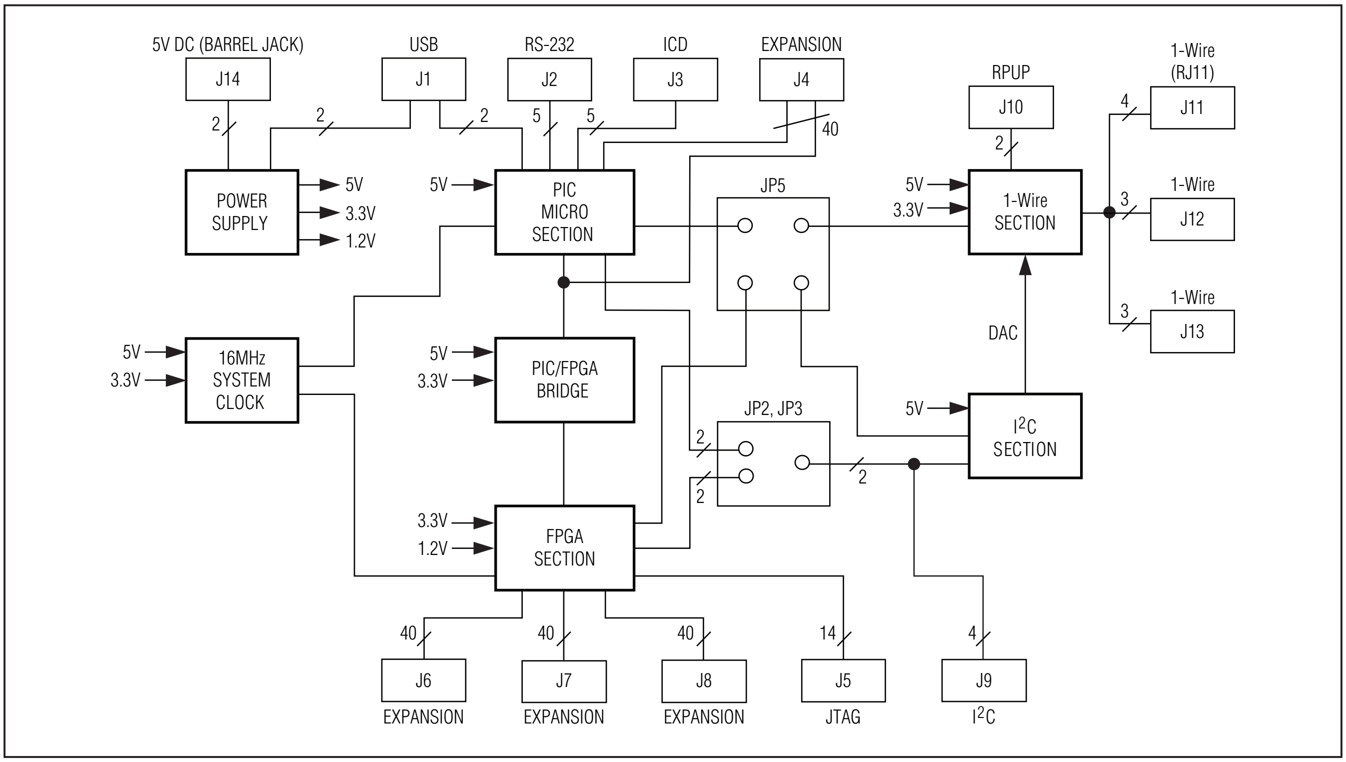

Figure 2. Secure Authentication Starter Kit Block Diagram

Detailed Description of Hardware

Figure 1 shows the starter kit with an overlaid grid to provide a quick reference for component location on the board. The block diagram in Figure 2 shows the circuit with all connectors and ports. Subsequent sections discuss the individual blocks, explain the necessary jumper settings, and give further references on additional applications of the board.

Power-Supply Section

The power-supply section contains three integrated circuits: U24, U25, and U26. U24 and U25 are step-down DC-DC converters that generate 3.3V and 1.2V from the 5V input voltage. U26 monitors and sequences the power lines and issues a reset pulse on power-on, when the 3.3V or 1.2V rail fails, or when the RESET POWER button (SW8) is pressed (user reset). The red LED (D9) is on if the 5V power is available. Power is supplied either from an external 5V ±5% source connected to J14 or the power line of the USB port (J1). See Table 1 for J14 pin assignments. Jumper JP9 must be installed according to the available power source. See the *Setting the Jumpers* section for details. Various test points give access to the 5V input and the 3.3V and 1.2V rails. TP8/TP9 and TP10/TP11 connect to 10mΩ resistors in the 3.3V and 1.2V rail to allow measuring the load current. A voltage measurement of 10mV corresponds to a current load of 1mA.

Table 1. J14 Pin Assignments

PIN	SIGNAL NAME	ALIAS
1	POWER	TIP
2	GND	RING
3	GND	RING
4	POWER	TIP

Note: *J14 has no printed pin 1 marker. Pin 1 is to the left of TP5. The pin numbering is counterclockwise.* ***Warning: Incorrect voltage applied to J14 can result in damage to the board.***

Table 2. J1 USB Port Pin Assignments

PIN	SIGNAL NAME
1	VBUS
2	USB DM
3	USB DP
4	NC
5–9	GND

Note: *J1 has no printed pin 1 marker. Pin 5 is above the right side of FB1. The pin numbering is descending left to right. Pins 6–9 are the outer part of the USB socket and connect to GND.*

Table 3. J2 RS-232 Port Pin Assignments

PIN	SIGNAL NAME	PIC PIN
1, 4, 6, 9	NC	—
2	T1OUT\	TX
3	R1IN	RX
5	GND	—
7	R2IN	RA3
8	T2OUT\	RA2

Note: *J2 has no printed pin 1 marker. Pin 1 is on the left side. The pin numbering is ascending left to right with pins 1 to 5 in the front row (accessible) and pins 6–9 in the rear row (not accessible).*

Table 4. J3 ICD Port Pin Assignments

PIN	SIGNAL NAME
1	RSTZ
2	5V
3	GND
4	PGD
5	PGC

Note: *J3 has no printed pin 1 marker. Pin 1 is labeled RSTZ. The pin numbering is ascending left to right.*

System Clock Section

The system clock section contains three integrated circuits: U21, U22, and U23. The clock source is U22, a 16MHz silicon oscillator. U21 and U23 are Schmitt-trigger inverters used as line drivers. U21, which is powered from the 5V supply, delivers a 5V clock signal to the PIC micro. U23 delivers a 3.3V clock signal to the FPGA. U22 and U23 operate on the 3.3V supply. There are no direct test points for the clock signal. The 5V clock can be probed at pin 39 of J4.

Table 5. J4 Expansion Port Pin Assignments

PIN	SIGNAL NAME		PIN	SIGNAL NAME
1	GND		2	OWSP
3	3V		4	RA2
5	OW		6	RST
7	5V		8	RB7
9	GND		10	RB6
11	RB5		12	RB4
13	RB3		14	RB2
15	SCL		16	SDA
17	RD7		18	RD6
19	RD5		20	RD4
21	RC7		22	RC6
23	USBP		24	USBM
25	RD3		26	RD2
27	RD1		28	RD0
29	RC2		30	RC1
31	RC0		32	RA6
33	RE2		34	RE1
35	RE0		36	RA5
37	RA4		38	RA3
39	CLKA		40	GND

PIC Micro Section

The PIC micro section contains two integrated circuits, the dual-channel RS-232 driver/receiver U2 and the microcontroller U5. Both U2 and U5 operate on the 5V supply. U2 makes the microcontroller accessible though a RS-232 port J2. The USB port J1 directly connects to the microcontroller. The ICD port J3 can be used to operate the microcontroller under the control of an in-circuit debugger. The expansion port J4 allows connecting external circuitry to the microcontroller. See Tables 2–5 for J1–J4 pin assignments. There are two pushbuttons (SW1, SW2) and two green LEDs (D1, D2) for user input and feedback. Their function depends on the software loaded into the microcontroller. The only jumper in the PIC micro section is JP4. It is relevant when the microcontroller functions as 1-Wire master. JP4 must be installed if the software-controlled 1-Wire power-delivery feature “strong pullup” is used. See the *Setting the Jumpers* section for details. There are no direct test points in the PIC micro section, however, several signals can be probed at J4.

FPGA Section

The FPGA section contains five integrated circuits: U10, U11, U12, U17, and U19. U10 and U12 are the FPGA and the associated JTAG PROM. U17 and U19 are level translators that allow the 3.3V FPGA to communicate with the 5V I^2C and 1-Wire section. The dual-input AND gate U11 implements a manual reset of the FPGA through SW7, independent of the power-on reset. The FPGA requires both 1.2V and 3.3V for operation. U11 runs on 3.3V. U17 needs 3.3V and 5V. U19 operates with 3.3V on the FPGA side and the user-selectable VPUP (JP10, JP11) on the 1-Wire side. The FPGA section has a JTAG port J5 and three expansion ports, J6, J7, and J8. See Tables 6–9 for the respective pin assignments. Besides the RESET button (SW7), the FPGA section has four more pushbuttons (SW3–SW6) and four green LEDs (D3–D6) for user input and feedback. Their function depends on the software loaded into the FPGA. The blue LED D7 reports the state of the FPGA's DONE signal. The LED is on if DONE is high. The FPGA section includes three jumpers: JP1, JB1, and JP6. JP1 relates to the FPGA suspend mode, which can be enabled to save power. JB1 controls whether the FPGA loads its configuration from U12 (normal operation) or from the JTAG port (during program development). JP6 is relevant when the FPGA functions as 1-Wire master. JP6 must be installed if the software-controlled 1-Wire power-delivery feature "strong pullup" is used. See the *Setting the Jumpers* section for details. There are no direct test points in the FPGA section.

Table 6. J5 JTAG Port Pin Assignments

PIN	SIGNAL NAME		PIN	SIGNAL NAME
1	GND		2	3V
3	GND		4	TMS
5	GND		6	TCK
7	GND		8	TDO
9	GND		10	TDI
11	GND		12	NC
13	GND		14	NC

Note: *J5 has no printed pin 1 marker. Pin 1 is on bottom right side of J5, and pin 2 is at the bottom left side. The odd numbers are on the right side ascending from bottom up. The even numbers are on the left side, ascending from bottom up.*

Table 7. J6 Bank 3 Expansion Port Pin Assignments

CONNECTOR PIN	FPGA PIN	SIGNAL NAME		CONNECTOR PIN	FPGA PIN	SIGNAL NAME
1	—	GND		2	—	5V
3	—	3V		4	C2	BANK3 IO2
5	C1	BANK3 IO1		6	D1	BANK3 IO4
7	E3	BANK3 IO3		8	E2	BANK3 IO6
9	F3	BANK3 IO5		10	E1	BANK3 IO8
11	H5	BANK3 IO7		12	F1	BANK3 IO10
13	G4	BANK3 IO9		14	G3	BANK3 IO12
15	J6	BANK3 IO11		16	G1	BANK3 IO14
17	H3	BANK3 IO13		18	G2	BANK3 IO16
19	H1	BANK3 IO15		20	H4	BANK3 IO18
21	J2	BANK3 IO17		22	J4	BANK3 IO20
23	J1	BANK3 IO19		24	K1	BANK3 IO22
25	K3	BANK3 IO21		26	L3	BANK3 IO24
27	J3	BANK3 IO23		28	L1	BANK3 IO26
29	L2	BANK3 IO25		30	K4	BANK3 IO28
31	M1	BANK3 IO27		32	L4	BANK3 IO30
33	M3	BANK3 IO29		34	M4	BANK3 IO32
35	N1	BANK3 IO31		36	N3	BANK3 IO34
37	N2	BANK3 IO33		38	P1	BANK3 IO35
39	—	GND		40	—	GND

Table 8. J7 Bank 0 Expansion Port Pin Assignments

CONNECTOR PIN	FPGA PIN	SIGNAL NAME		CONNECTOR PIN	FPGA PIN	SIGNAL NAME
1	—	GND		2	—	5V
3	—	3V		4	C4	BANK0 IO2
5	A14	BANK0 IO1		6	B14	BANK0 IO4
7	A13	BANK0 IO3		8	D13	BANK0 IO6
9	C13	BANK0 IO5		10	C12	BANK0 IO8
11	A12	BANK0 IO7		12	D11	BANK0 IO10
13	B12	BANK0 IO9		14	C11	BANK0 IO12
15	A11	BANK0 IO11		16	D10	BANK0 IO14
17	A10	BANK0 IO13		18	E10	BANK0 IO16
19	A9	BANK0 IO15		20	D9	BANK0 IO18
21	C9	BANK0 IO17		22	C8	BANK0 IO20
23	A8	BANK0 IO19		24	E7	BANK0 IO22
25	B8	BANK0 IO21		26	D8	BANK0 IO24
27	A7	BANK0 IO23		28	D7	BANK0 IO26
29	C7	BANK0 IO25		30	C6	BANK0 IO28
31	A6	BANK0 IO27		32	C5	BANK0 IO30
33	B6	BANK0 IO29		34	D4	BANK3 IO37
35	A5	BANK0 IO31		36	B4	BANK0 IO32
37	C16	BANK1 IO36		38	D3	BANK3 IO36
39	—	GND		40	—	GND

Table 9. J8 Bank 1 Expansion Port Pin Assignments

CONNECTOR PIN	FPGA PIN	SIGNAL NAME		CONNECTOR PIN	FPGA PIN	SIGNAL NAME
1	—	GND		2	—	5V
3	—	3V		4	N13	BANK1 IO2
5	N14	BANK1 IO1		6	N16	BANK1 IO4
7	R15	BANK1 IO3		8	M13	BANK1 IO6
9	M14	BANK1 IO5		10	L13	BANK1 IO8
11	K13	BANK1 IO7		12	M15	BANK1 IO10
13	M16	BANK1 IO9		14	L14	BANK1 IO12
15	L16	BANK1 IO11		16	K15	BANK1 IO14
17	J13	BANK1 IO13		18	K16	BANK1 IO16
19	J14	BANK1 IO15		20	J16	BANK1 IO18
21	H15	BANK1 IO17		22	H16	BANK1 IO20
23	H13	BANK1 IO19		24	G16	BANK1 IO22
25	H14	BANK1 IO21		26	G14	BANK1 IO24
27	G13	BANK1 IO23		28	F16	BANK1 IO26
29	F15	BANK1 IO25		30	E16	BANK1 IO28
31	F14	BANK1 IO27		32	E14	BANK1 IO30
33	F13	BANK1 IO29		34	D16	BANK1 IO32
35	D15	BANK1 IO31		36	E13	BANK1 IO34
37	D14	BANK1 IO33		38	C15	BANK1 IO35
39	—	GND		40	—	GND

PIC/FPGA Bridge Section

The PIC/FPGA bridge section contains seven integrated circuits: U1, U3, U4, and U6–U9. U6 and U7 transfer and level-translate address and data signals between the PIC and the FPGA. U1, U3, U8, and U9 level-convert control signals from the PIC to U6, U7 and the FPGA from 5V to 3.3V levels. U4 level-converts a feedback signal of the FPGA from 3.3V to 5V. Besides U4, which runs on 5V, the other integrated circuits of the PIC/FPGA bridge operate on 3.3V. The only test point in the bridge is TP1, which allows access to the signals that controls write access to the FPGA.

Table 10. J9 I²C Expansion Port Pin Assignments

PIN	SIGNAL NAME
1	5V
2	SCL
3	SDA
4	GND

Table 11. J10 RPUP Socket Pin Assignments

PIN	SIGNAL NAME
1	VPUP
2	OW

Table 12. J11 RJ11 Port Pin Assignments

PIN	SIGNAL NAME
1	5V
2	GND
3	OW (DATA)
4	OW RTN
5	NC
6	NC

Note: *J11 has no printed pin 1 marker. Pin 1 is at the bottom. The pin numbering is ascending from bottom to top.*

I²C Section

The I²C section contains four integrated circuits: U13–U16. U13 is a 1-Wire master, which can be selected by JP5 to communicate with 1-Wire devices on or external to the board. U14 is a 1Kb I²C/SMBus EEPROM with SHA-1 engine and U15 is a SHA-1 coprocessor. These are the typical I²C devices to be evaluated with this board. U16 is the DAC to generate the adjustable 1-Wire pullup voltage. J9 is intended for connecting a small circuit board with an I²C slave. See Table 10 for the pin assignments. The I²C section includes the jumpers JP2, JP3, and JP8. JP2 and JP3 must be populated with one jumper each to select either the PIC micro or the FPGA as I²C master. JP8 is relevant when the DS2482-100 functions as 1-Wire master. JP8 should be installed if the software-controlled 1-Wire power-delivery feature "strong pullup" is used. See the *Setting the Jumpers* section for details. The I²C section has two test points (TP2, TP3) that allow monitoring the activity on SCL and SDA.

1-Wire Section

The 1-Wire section contains two integrated circuits: U18 and U20. U18 is an ESD protection device, which protects the 1-Wire section from ESD hits that could be introduced at J11, J12, or J13. U20 is a 1Kb protected 1-Wire EEPROM with SHA-1 engine, which can be put on the 1-Wire bus using JP7. Special attention is necessary for J10. Because the R37 position is not populated, it is necessary to install a pullup resistor to the 1-Wire bus across the terminals of J10. The typical pullup resistor value is 2.2kΩ. The resistor must not be installed when using the DS2482-100 as 1-Wire master. J11 allows connecting DS1402 1-Wire network cables to the 1-Wire bus. It can also be used to access U20 from the outside, provided that the terminals of J10 are open, and no jumper is installed at JP5. J12 is intended for connecting a small circuit board with a 1-Wire slave. A 1-Wire slave in a TO-92 or PR-35 package can directly be inserted at J13. See Tables 11–14 for the respective pin assignments. Besides JP7, the 1-Wire section includes the jumpers JP5, JP10, and JP11. JP5 must be populated with one

Table 13. J12 1-Wire Expansion Port Pin Assignments

PIN	SIGNAL NAME
1	GND
2	3V
3	OW

Table 14. J13 TO-92 Socket Pin Assignments

PIN	SIGNAL NAME
1	GND
2	OW
3	GND

jumper to select either the PIC micro, or the FPGA or the DS2482-100 as 1-Wire master. JP10 must be populated to select the 1-Wire pullup voltage, which is typically 5V or 3.3V. JP11 is intended to select a user-programmable pullup voltage, which is controlled by U16, a digital-to-analog converter in the I2C section. As a factory setting, the JP11 location is not populated and the FIXED VPUP selection is hardwired by means of a short (R51). To use adjustable VPUP, R51 must be removed and JP11 must be populated. For more details see the *Setting the Jumpers* section. The 1-Wire section has three test points: TP4, TP12, and TP13. TP4 allows monitoring the activity on the 1-Wire bus. TP12 and TP13 connect to a 10ml resistor in the VPUP path, which allows measuring the load current. A voltage measurement of 10mV corresponds to a current load of 1mA.

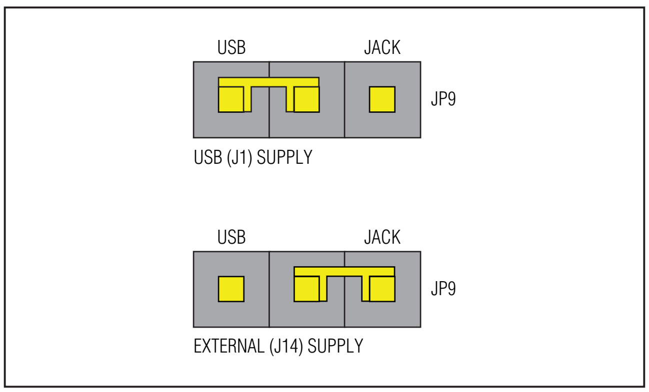

Figure 3. JP9, Power Source Selection

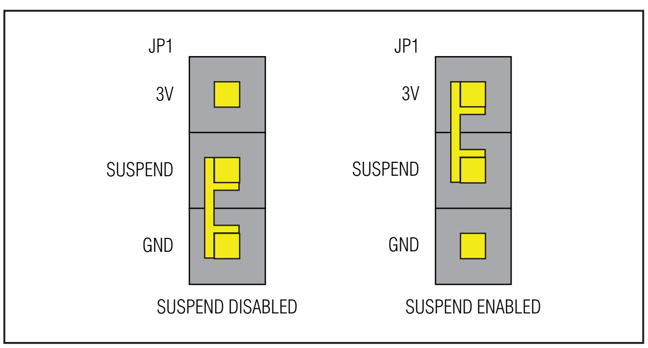

Figure 4. JP1, Suspend Mode Selection

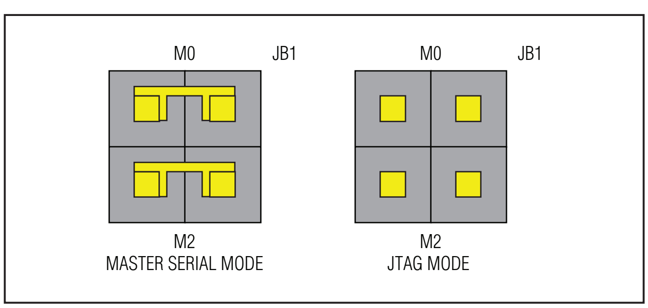

Figure 5. JB1, FPGA Configuration Source Selection

Setting the Jumpers

Power Supply

Jumpers must be installed according to the available power source. See Figure 3.

FPGA Suspend Mode

The suspend mode, if enabled, reduces power consumption (Figure 4). Refer to XAPP480 for more information.

FPGA Initialization

In master-serial mode, the FPGA loads its configuration from U12 (PROM). This setting is used for normal operation. In JTAG mode, the FPGA loads its configuration from the JTAG interface J5. This setting is used for FPGA program development. Configurations with only one jumper (M0 or M2) installed are not valid. See Figure 5.

I2C Master Selection

Both jumpers must be installed as shown in Figure 6, either to select the PIC or the FPGA.

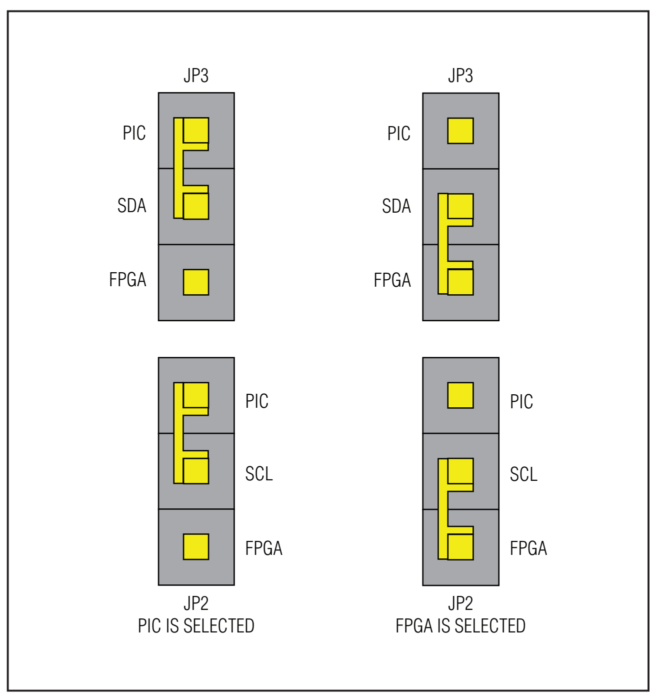

Figure 6. JP2, JP3, I2C Master Selection

1-Wire Master Selection

With the DS2482-100 or an external master, the resistor at J10 must be removed. See Figure 7.

1-Wire Pullup Voltage Selection

JP10 defines the 1-Wire pullup voltage unless adjustable pullup voltage is selected. See Figure 8 for details.

1-Wire Strong Pullup Enable

Strong pullup must be enabled when using the PIC or FPGA to operate 1-Wire slaves that temporarily enter a high-power mode. The DS2482-100 has a built-in strong pullup, therefore, the strong pullup enable is optional. See Figure 9.

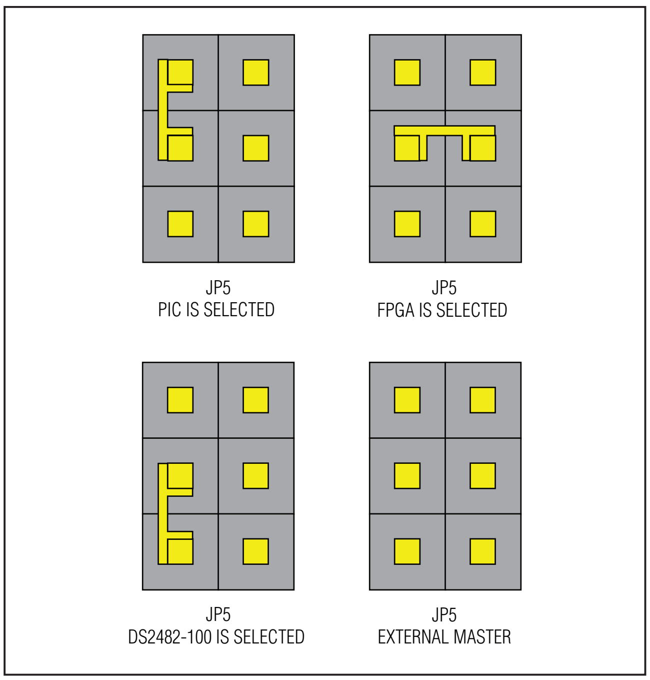

Figure 7. JP5, 1-Wire Master Selection

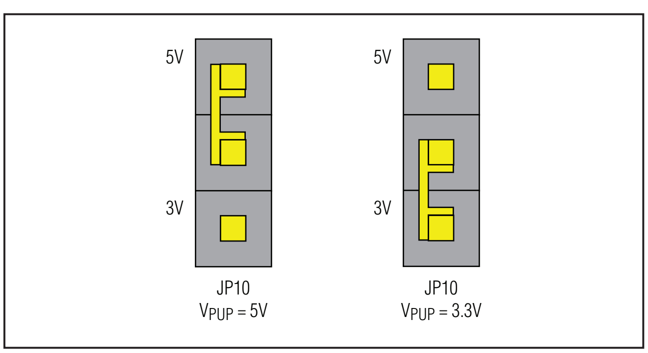

Figure 8. JP10, 1-Wire Pullup Voltage preselection

DS28E01 Access

To access the DS28E01, the jumper must be installed. See Figure 10.

Adjustable 1-Wire Pullup Voltage

JP11 is not factory installed. To use JP11, R51 must be removed. See Figure 11.

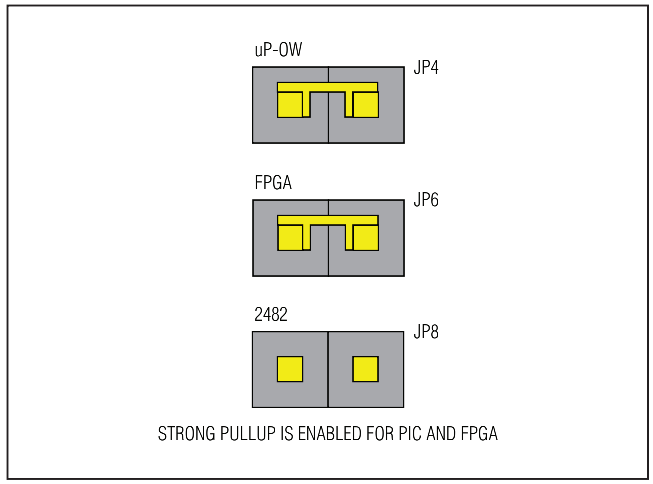

Figure 9. JP4, JP6, JP8, 1-Wire Strong Pullup Enable

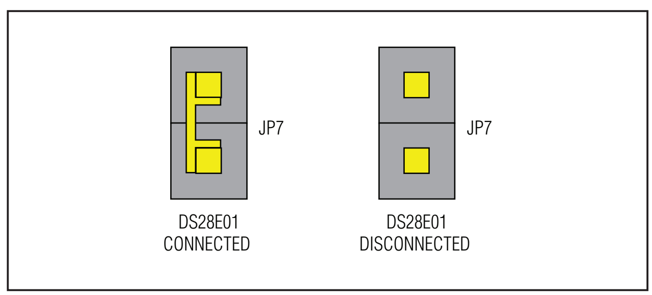

Figure 10. JP7, DS28E01 Access

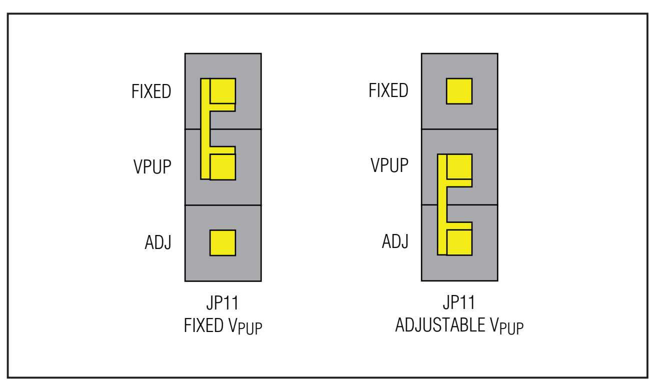

Figure 11. JP11, Fixed vs. Adjustable 1-Wire Pullup Selection

Supported Configurations

The challenge and response authentication can be implemented relying solely on the PIC or the FPGA. The PIC can communicate to the FPGA by means of a 6-bit address bus, 8-bit data bus, and control lines. This way firmware in the PIC can offload some functions to the FPGA. The FPGA can contain the DS1WM synthesizable 1-Wire bus master, the DSSHA1 processor together with the user's FPGA design to create a custom security solution. The SHA-1 computation can be performed by PIC software, the FPGA (DSSHA1), or the DS2460 SHA-1 coprocessor. The 1-Wire bus can be driven directly, i.e., from the PIC, the FPGA (DS1WM), or the DS2482-100. The I^{2}C bus can be driven by the PIC through its built-in I^{2}C port or by the FPGA (I2CM). Table 15 shows the possible combinations supported by the secure authentication starter kit.

Additional Applications of the Secure Authentication Starter Kit

Using the PIC with RS-232

A standard female DB9 connector (J2), along with a line transceiver/receiver (U2), provides an RS-232 serial connection to the demonstration board. This serial connection can be used by the programmer to develop communication with Windows®, Linux®, and Mac OS® operating systems or other types of serial-capable host systems. This is one of the more traditional and usually simpler ways of establishing communication to a serial-capable host system. An additional advantage the serial port provides is that most computers contain a terminal program that supports communication to a serial port. In doing so, the developer can write his firmware in the PIC as to not need any software installed on computers across many operating systems.

Table 15. Configurations Overview

HOST	SHA-1 COMPUTATION	BUS INTERFACE	PATH	TARGET SLAVE DEVICE
PIC alone	**Software code (PIC)** or DS2460 (PIC I^{2}C port)	1-Wire Software code (PIC)	Direct	DS28E01 (1-Wire)
		I^{2}C (PIC I^{2}C port)	By DS2482-100	
			Direct	**DS28CN01 (I^{2}C)**
PIC with FPGA	Software code (PIC) or DSSHA1 (Verilog, FPGA) or DS2460 (PIC I^{2}C port)	1-Wire Software code (PIC) or DS1WM (VHDL/Verilog, FPGA)	Direct	DS28E01 (1-Wire)
		I^{2}C (PIC I^{2}C port)	By DS2482-100	
			Direct	DS28CN01 (I^{2}C)
FPGA alone	PicoBlaze™ ASM code (FPGA) or DSSHA1 (Verilog, FPGA) or DS2460 (FPGA I2CM*)	1-Wire PicoBlaze ASM code (FPGA) or DS1WM (VHDL/Verilog, FPGA)	Direct	DS28E01 (1-Wire)
		I^{2}C I2CM* (VHDL, FPGA)	By DS2482-100	
			Direct	DS28CN01 (I^{2}C)

**I2CM is in development.*

Note: *The board hardware supports all permutations indicated in Table 15. Some combinations are of more interest than others. The example implementation in bold indicates PIC alone with SHA-1 computation in software using the I^{2}C port of the PIC to communicate directly to the DS28CN01.*

Windows is a registered trademark of Microsoft Corp.
Linux is a registered trademark of Linus Torvalds.
Mac OS is a registered trademark of Apple Inc.
PicoBlaze is a trademark of Xilinx, Inc.

Secure Authentication Starter Kit

Using PIC with USB Port

In addition to the USB port (J1) being able to supply power to the board, the USB port also connects to the PIC. The USB port can be used to develop USB-based applications intended to interface with Windows OS, Linux, Mac OS, or other types of USB-capable host systems. This is meant to be an alternative to using the serial connection and can be essential in today's market as serial cable host systems continue to diminish and USB-capable host systems increases. Additionally, it is possible to develop a USB functional bootloader inside the PIC to provide field firmware updates as needed by a company's customer base.

Debugging and Updating the PIC Firmware

The PIC microcontroller can be debugged and updated with firmware by the ICD port (J3). The ICD port supports Microchip's MPLAB® ICD 3 In-Circuit Debugger with a PC that contains the MPLAB IDE software. By using this ICD port, the programmer can load development code, set break points, step through code to verify correct operation, and test/erase firmware.

Changing the FPGA Configuration

The Xilinx Spartan-3A FPGA is to be configured by the JTAG port (J5). The JTAG port supports the HW-USB-II-G (Platform Cable USB II) or other Xilinx cables to program the FPGA directly or to program the available XCF04S JTAG PROM. A 14-position, 2mm ribbon cable can be connected from the HW-USB-II-G to the JTAG port. The free software to perform the programming is integrated with the Xilinx ISE® WebPACK® software called iMPACT. Refer to the Xilinx website for more information. Figure 12 shows the actual JTAG chain. The FPGA or the JTAG PROM can be directly loaded in the chain. When using the JTAG PROM, the user also needs to install both jumpers located at JB1 for the FPGA to actually get loaded.

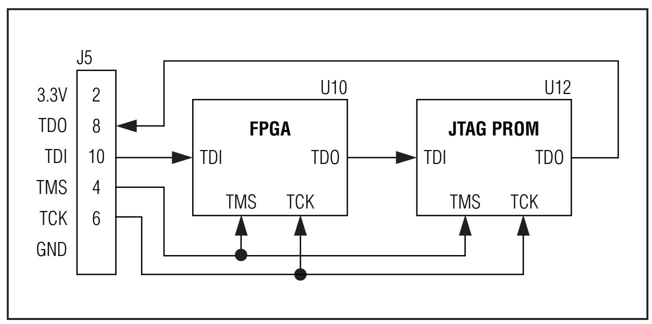

Figure 12. JTAG Chain Topology

MPLAB is a registered trademark of Microchip Technology Inc.

ISE and WebPACK are registered trademarks of Xilinx, Inc.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	6/11	Initial release	—