参考資料

TI Designs: TIDEP-0093
電子販売時点管理(EPOS)支払い端末リファレンス・デザイン

概要

TIDEP-0093デザインは、PCI-PTSおよびEMV要件への適合に役立つプロセッサにより、迅速な製品化を可能にします。電子販売時点管理(EPOS)支払い端末には、認証付きブート、不正検出、DDR暗号化などの機能が必要です。AM438xプロセッサを使用すると、Payment Card Industry (PCI)認証に適合するシステム設計が可能になります。スケーラビリティに優れたAM438xプロセッサは、各種プロセッサ速度とローエンドからハイエンドまでのアプリケーションに対応するソフトウェアに加えて、スマート・カードや磁気カード・リーダーなどの、支払い端末で必要とされる主要ペリフェラルを含む十分な接続機能を提供します。

リソース

TIDEP-0093	デザイン・フォルダ
AM438x	プロダクト・フォルダ
TPS65218	プロダクト・フォルダ
TCA5013	プロダクト・フォルダ

TI E2E™ Community

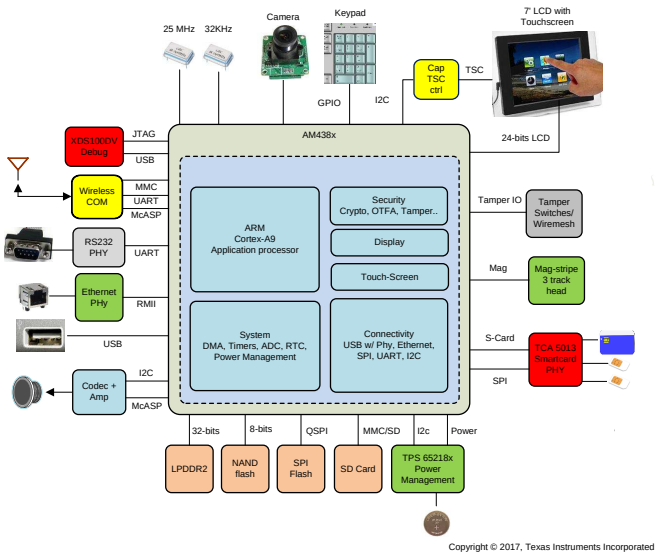
E2Eエキスパートに質問

特長

- TI Sitara™AM438xプロセッサと、販売時点管理アプリケーションの設計に役立つ内蔵機能
- ARM® Cortex®-A9ベースのプロセッサ、300MHz、600MHz、1GHzの各種速度、3Dグラフィックおよび PRUオプション付き
- Linux®開発用のプロセッサ・ソフトウェア開発キット（SDK）
- スマート・カードおよび磁気カード・リーダーと、タッチスクリーン・ディスプレイ、キーパッド、USB、イーサネットなどのペリフェラル
- TI TPS65218電源管理ICおよびTCA5013スマート・カードPHYデバイスを搭載

アプリケーション

- 自動販売機、精算機、両替機
- ハンドヘルドおよび据え置き型EFT端末
- EPOS、ECR、レジ
- 給油機
- EPOSプリンタ
- ATM



1 System Description

Based on the AM438x EVM, the TIDEP-0093 design is a kickstarter for customers wanting to design a module or system for EPOS. The TIDEP-0093 design uses the Sitara AM438x, TPS65218x, and TCA5013 devices.

The TI AM438x high-performance processors are based on the ARM Cortex-A9 core. The processors are enhanced with payment card peripherals and logical and physical security to help customers meet PCI requirements. The devices support high-level operating systems (HLOS). Linux is available free of charge from TI. The devices offer an upgrade to systems that are based on lower-performance ARM cores, provide updated peripherals (including memory options such as QSPI-NOR and LPDDR2), and support the security features typically required for PCI-PTS. AM438x integrates key peripherals often required in payment terminals: smart card reader and magnetic card reader. 図 1 shows the Sitara AM438x.

図 1. Sitara AM438x

The TPS65218x is a power management solution for AM438x with special rails to power AM438x's tamper module. The TPS65218x provides three step-down converters, three load switches, three general-purpose IOs, two battery backup supplies, one buck-boost converter, and one low-dropout (LDO) regulator. The system can be supplied by a single-cell Li-Ion battery or regulated 5-V supply. A coin-cell battery can be added to supply the two always-on backup supplies. 図 2 shows the TPS65218x.

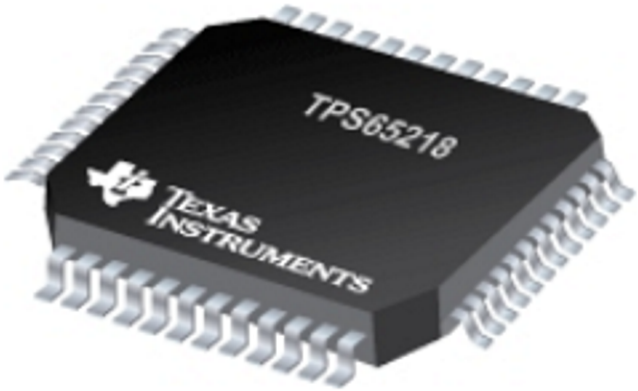


図 2. TPS65218x

The TCA5013 is designed to seamlessly work with AM438x. The TCA5013 is a smart card interface IC that is targeted for use in point of sale (POS) terminals. The device enables POS terminals to interface with EMV4.3, ISO7816-3, and ISO7816-10 compliant cards. The device supports up to three secure access module (SAM) cards in addition to one user card. 図 3 shows the TCA5013.

図 3. TCA5013

2 System Overview

2.1 Block Diagram

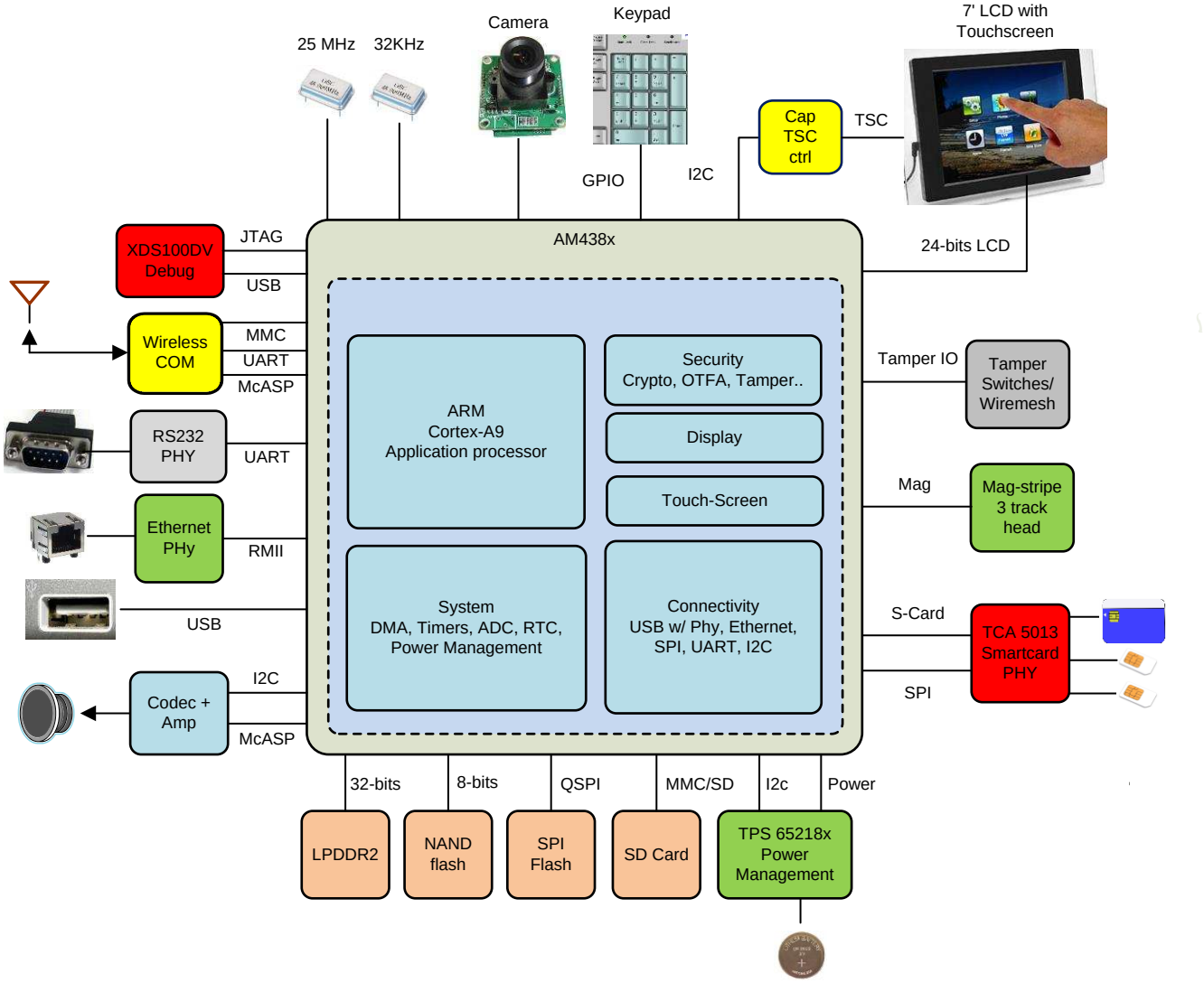


図 4. EPOS EVM System Block Diagram

2.2 Highlighted Products

2.2.1 AM438x

The TI AM438x high-performance processors are based on the ARM Cortex-A9 core. The processors are enhanced with payment card peripherals and logical and physical security to help customers meet payment card industry (PCI) requirements.

The devices support HLOS. Linux is available free of charge from TI. The devices offer an upgrade to systems that are based on lower-performance ARM cores, provide updated peripherals (including memory options such as QSPI-NOR and LPDDR2), and support the security features discussed in this design guide.

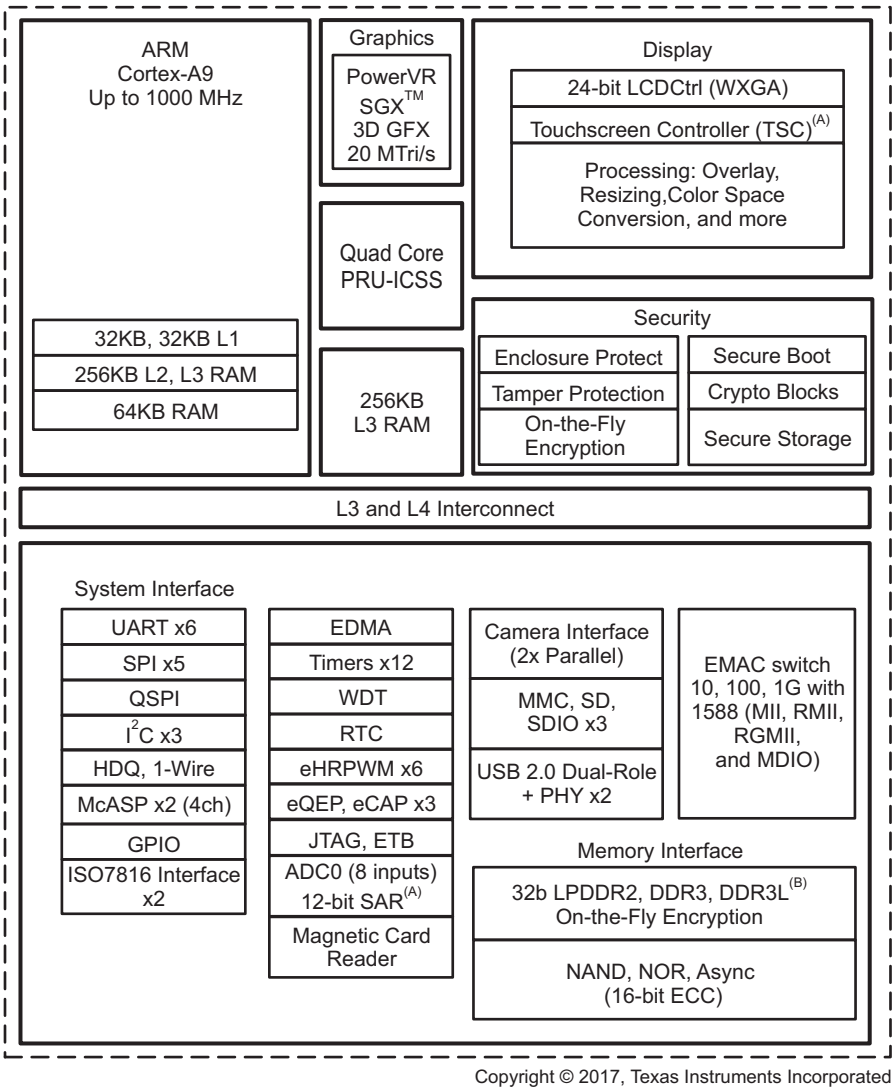


図 5. AM438x Functional Block Diagram

The processor subsystem is based on the ARM Cortex-A9 core, and the PowerVR SGX™ graphics accelerator subsystem provides 3D graphics acceleration to support display and advanced user interfaces.

The programmable real-time unit subsystem and industrial communication subsystem (PRU-ICSS) is separate from the ARM core and allows independent operation and clocking for greater efficiency and flexibility. The programmable nature of the PRU-ICSS, along with the system's access to pins, events, and all system-on-chip (SoC) resources, provides flexibility in implementing fast real-time responses, specialized data handling operations, custom peripheral interfaces, and in offloading tasks from the other processor cores of the SoC.

High-performance interconnects provide high-bandwidth data transfers for multiple initiators to the internal and external memory controllers and to on-chip peripherals. The device also offers a comprehensive clock-management scheme. The on-chip analog-to-digital converter (ADC0) can couple with the display subsystem to provide an integrated touch-screen solution. There is also an EMV-compliant ISO7816 interface (smart card) interface and magnetic card controller (ADC1).

The real-time clock (RTC) provides a clock reference on a separate power domain. The clock reference enables a battery-backed clock reference.

The camera interface offers configuration for a single- or dual-camera parallel port.

The physical protection subsystem adds enclosure protection to the secure features offered by the AM438x processors, which include cryptography acceleration and secure boot. Enclosure protection helps customers design products that detect when the casing is opened and protect sensitive parts of the circuit with a wire mesh. Tamper protection monitors voltage, temperature, and crystal frequency so system designers can detect external attacks.

In addition, the partial ARM TrustZone® technology allows system designers to configure memory for secure storage and protect against software attacks.

2.2.2 TPS65218x

The TPS65218x provides three step-down converters, three load switches, three general-purpose IOs, two battery backup supplies, one buck-boost converter, and one LDO. The system can be supplied by a single cell Li-Ion battery or regulated 5-V supply. A coin-cell battery can be added to supply the two always-on backup supplies. The device is characterized across a –40°C to 105°C temperature range, which makes it suitable for various industrial applications.

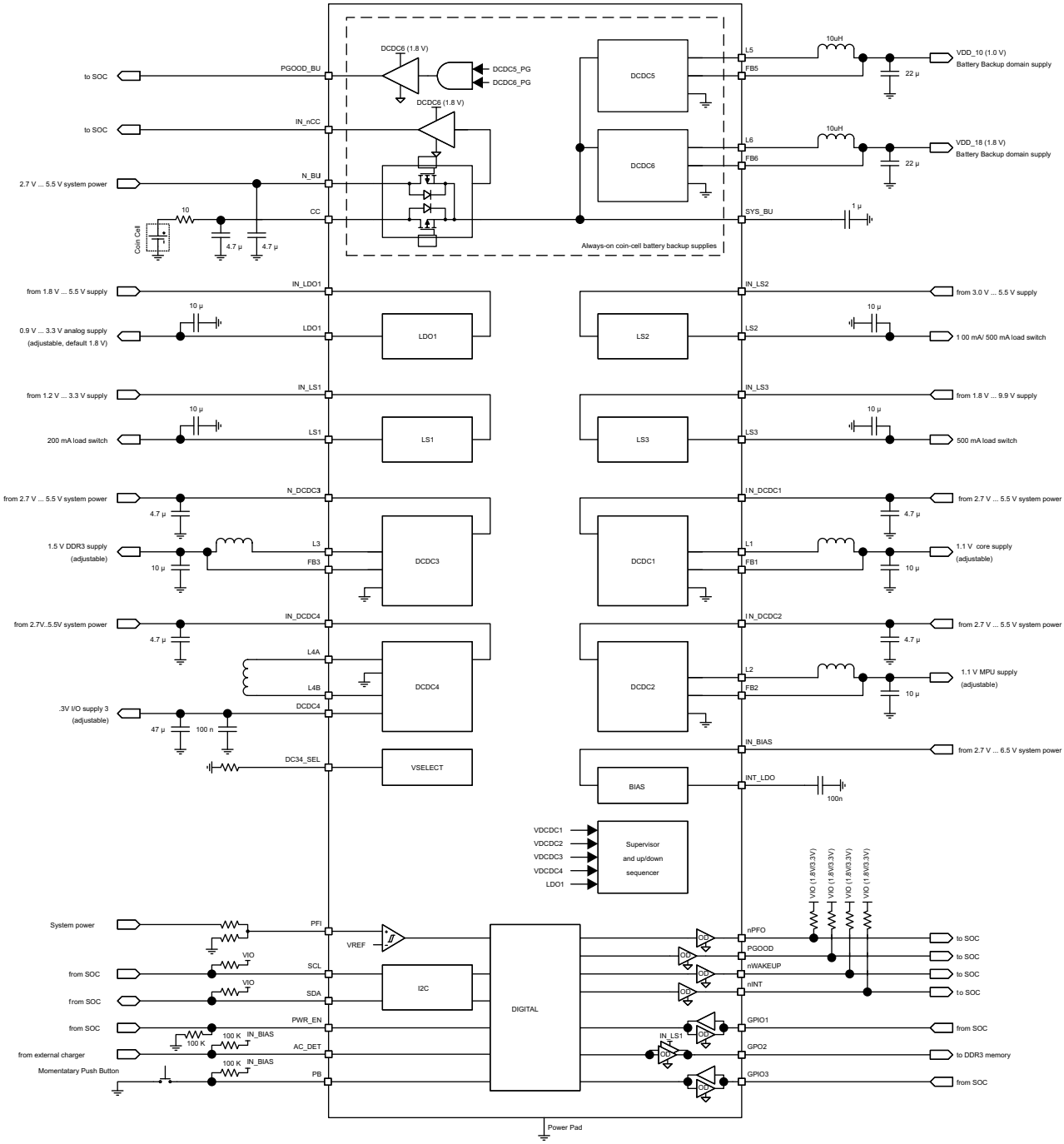


図 6. TPS65218x Functional Block Diagram

The I²C interface provides comprehensive features for using the TPS65218x. All rails, load-switches, and GPIOs can be enabled or disabled. Voltage thresholds for the undervoltage lockout (UVLO) and supervisor can be customized. Power-up and power-down sequences can also be programmed through I²C. Interrupts for overtemperature, overcurrent, and undervoltage can be monitored as well.

The integrated voltage supervisor monitors DC-DC 1 through 4 and LDO1. The supervisor has two settings; the standard settings only monitor for undervoltage while the strict settings implement tight tolerances on both undervoltage and overvoltage. A power good signal is provided to report the regulation state of the five rails.

The three hysteretic step-down converters can each supply up to 1.8 A of current. The default output voltages for each converter can be adjusted through the I²C interface. DC-DC 1 and 2 feature dynamic voltage scaling with adjustable slew rate. The step-down converters operate in a low power mode at light load and can be forced into PWM operation for noise sensitive applications.

The battery backup supplies consist of two low-power step-down converters optimized for very light loads and are monitored with a separate power good signal. The converters can be configured to operate as always-on supplies with the addition of a coin-cell battery. The state of the battery can be monitored over I²C.

2.2.3 TCA5013

The TCA5013 is a smart card interface IC that is targeted for use in POS terminals. The device enables POS terminals to interface with EMV4.3, ISO7816-3, and ISO7816-10 compliant cards. The device supports up to three SAM cards in addition to one user card.

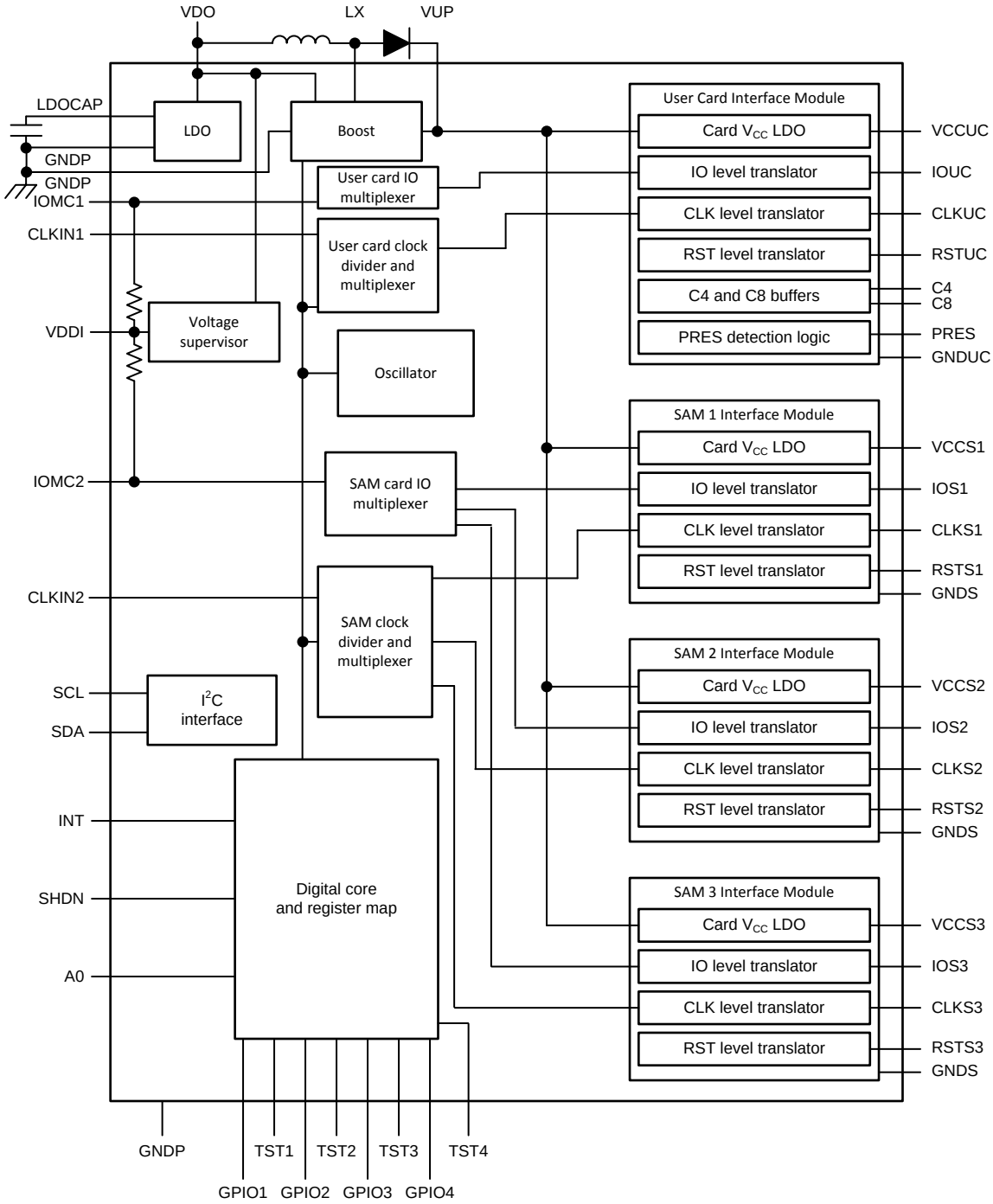


図 7. TCA5013 Functional Block Diagram

The TCA5013 operates from a single supply and generates all the card voltages. The device is controlled by a standard I^2C interface and is capable of card activation and deactivation per EMV4.3 and ISO7816-3 standards. In addition the device also supports ISO7816-10 synchronous cards. The TCA5013 has a 4-byte FIFO that stores the answer to reset (ATR) sequence in ISO7816-10 type one cards. Synchronous cards (ISO7816-10 type one and type two) can be set up for automatic activation or manual activation. The device has multiple power saving modes and also supports power saving in the smart card itself by *clock stop* or lowering clock frequency to lowest allowable levels per the ISO7816-3 standards.

The TCA5013 has IEC 61000-4-2, 8-kV, contact discharge on all pins that interface with smart cards, which enables the system to be resistant to ESD in the field without the requirement for external ESD devices. The device is available in a 5-mm×5-mm BGA package. All IO pins are securely surrounded by other pins in the pinout of the device, which prevents the secure pins from being probed during device operation.

3 Hardware, Software, Testing Requirements, and Test Results

3.1 Required Hardware and Software

3.1.1 Hardware

The AM438x EPOS evaluation module (EVM) is a standalone test, development, and EVM system that enables developers to write software and develop hardware around an AM438x processor subsystem. The EPOS EVM also hosts TPS65218 and TCA5013 devices.

See the *AM438x EPOS EVM Hardware's User's Guide*[2] for getting started instructions and details on hardware architecture of EPOS EVM.

The following hardware is required to get the smart card demonstration application:

- AM438x EPOS EVM
- SD card (the TI processor SDK EPOS image requires at least 8GB of space)
- Power supply (5 V, 3 A) for the AM438x-based board
- Programmed SMART card

注: The smart card demonstration application uses an ACOS3 demo card. This smart card is programmed with ACOS3 demo card Flash scripts.

3.1.2 Software

The AM438x EPOS SDK is a restricted-access software package that requires business approval and a special NDA with TI before access is provided from the TI secure delivery portal (mySecure Software). See 5 on how to request access.

Once access is given, the AM438x EPOS SDK package contains a software user's guide and additional documentation for setting up and running the demonstration test applications.

With the required hardware, perform the following steps to replicate the software portion of the demonstration.

For the purposes of this design guide, it is assumed that a Linux host machine is being used. Program the SD card with the Linux processor SDK image using the following steps:

1. Download the SDK installer ti-processor-sdk-am438x-epos-evm-xx.xx.xx.xx-Linux-x86-Install.bin from TI mySecure site (where "xx.xx.xx.xx" is the version number of the latest Linux Processor SDK EPOS).
2. Create the SD card with default images using the SDK Create SD Card Script or see the user's guide.
3. Boot the Linux kernel and file system using the created SD card.

3.2 Testing and Results

3.2.1 Test Setup

This section provides details of test setup with the required hardware and software to be able to run the TI EPOS software application.

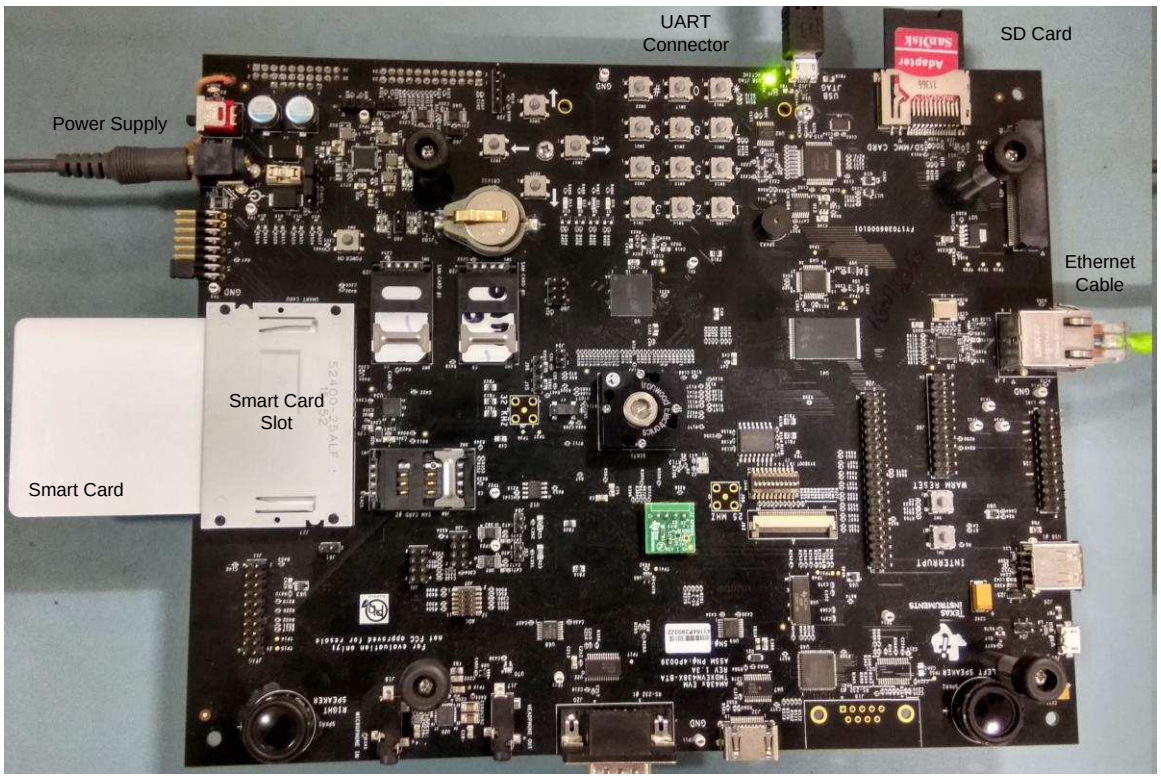


図 8. AM438x EVM Setup

3.2.2 Test Results

This section provides the test cases details and results for the TI smart card software application.

図 9. AM438x Default Matrix GUI

Test Case One: EPOS Smart Card Demo Application Launcher

1. On Matrix GUI, select the EPOS icon to launch the submenu (see 図 10).

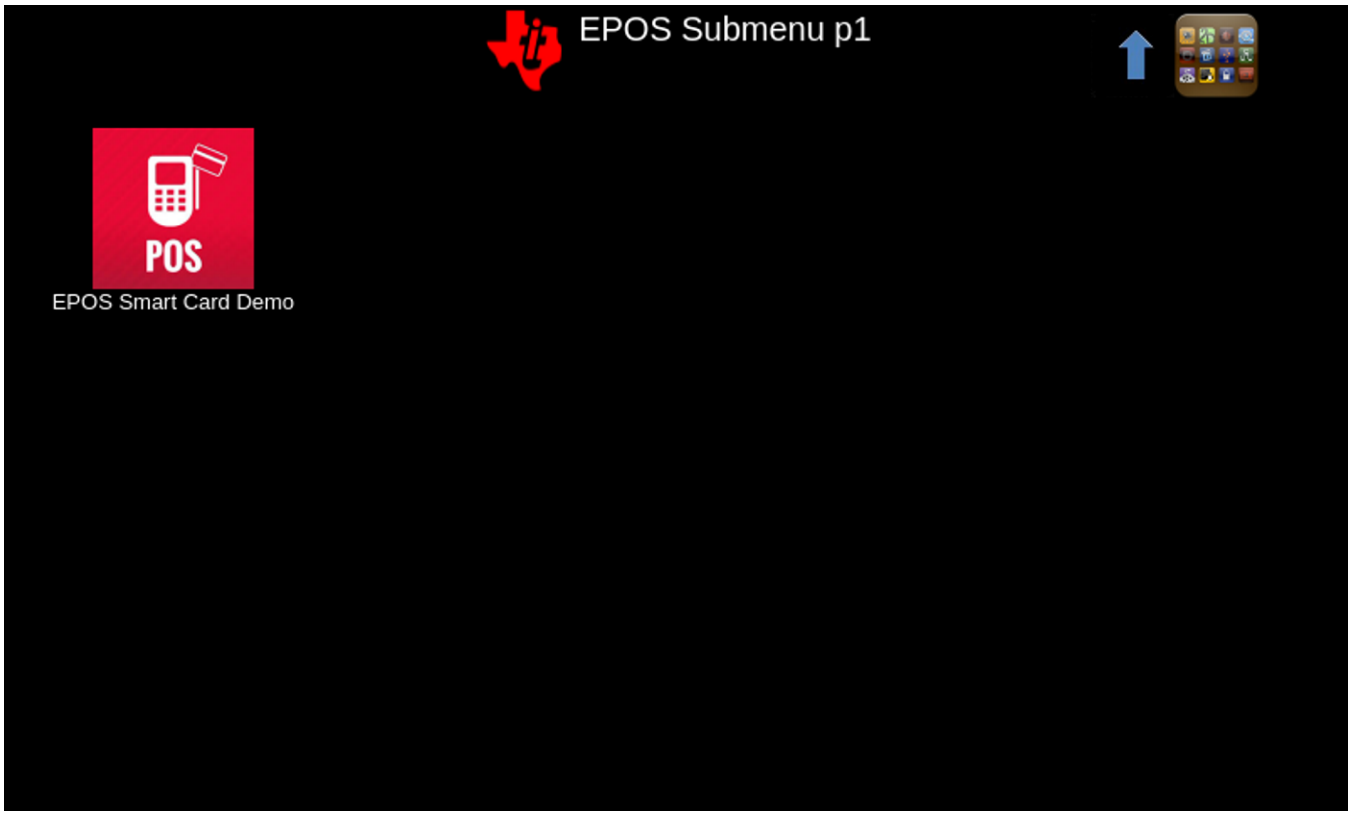


図 10. EPOS Submenu to Launch EPOS Smart Card Demo

2. Select the EPOS Smart Card Demo App *RUN* utility (see 図 11).

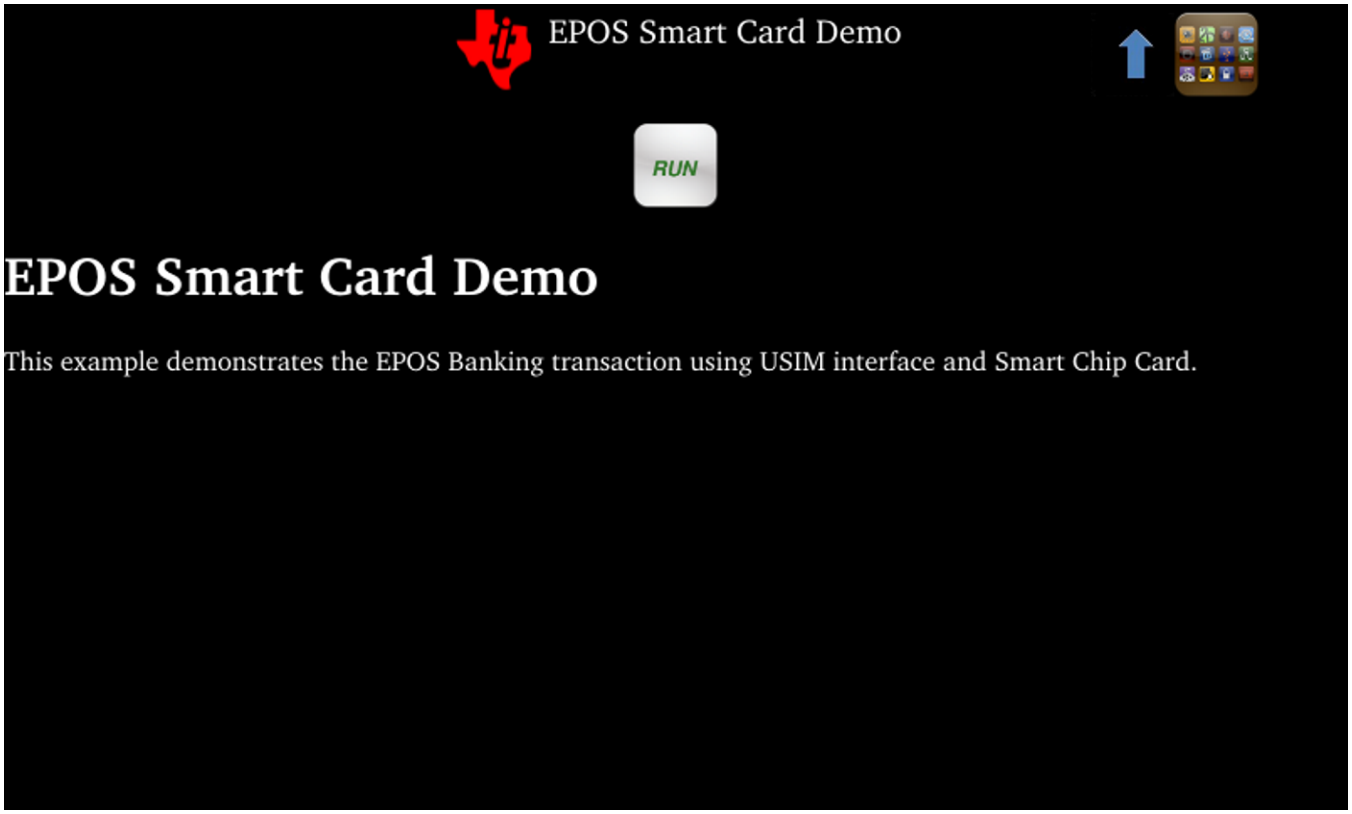


図 11. EPOS Smart Card Demo Home Screen

3. Result: TI EPOS Demo screen should launch (see 図 12).

図 12. EPOS Smart Card Demo Launch Successful

Test Case Two: Smart Card Detection

1. Insert preprogrammed smart card into the card slot.
2. Result: On successful card presence detection, the program redirects to the *authentication screen* in 図 13.

図 13. Authentication Screen

Test Case Three: Smart Card Authentication With PIN Validation

1. Enter the default PIN as 12345678.
2. Press the * key to enter.

注: Press the # key to cancel or re-enter the PIN.

図 14. PIN Authentication Login

3. Result: On successful PIN authentication, the TI EPOS Demo menu screen opens (see 図 15).

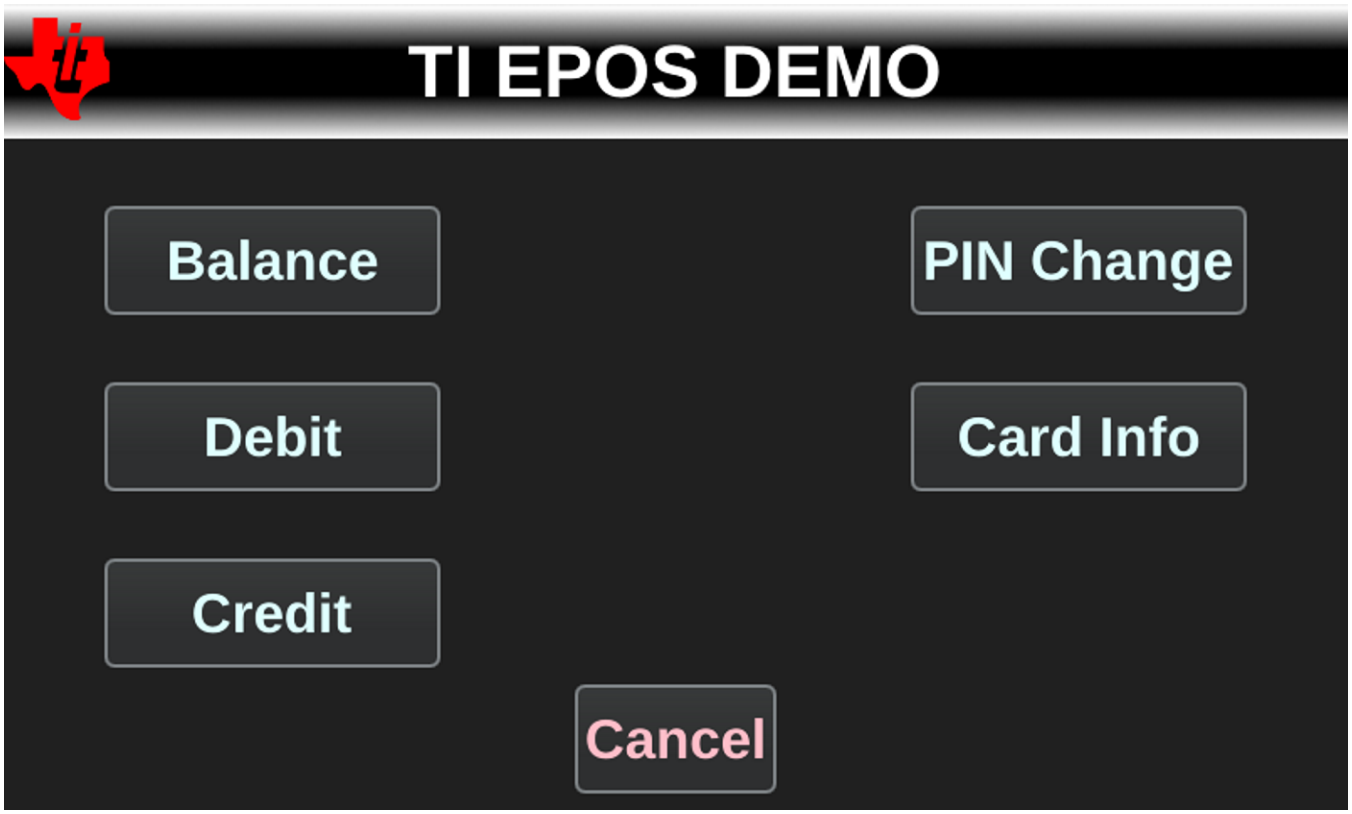


図 15. PIN Authentication Successful

注: An invalid PIN or pressing *Cancel* returns the user to the card detection screen.

Test Case Four: Smart Card Information

1. Select the *Card Info* icon for card information.
2. Select *OK* to return to the main menu.

3.2.2.1 Wire Mesh Tamper

A wire mesh is a loop between two PIOs—one acting as a TX and the other RX. When the RX stops receiving the TX signal, it generates a tamper event.

表 1. Wire Mesh Pin Configuration

SIGNAL NAME	HEADER	PIN	SIGNAL NAME	HEADER	PIN
TM_PIO_0	J34	5	TM_PIO_8	J34	11
TM_PIO_1		6	TM_PIO_9		12
TM_PIO_2		7	TM_PIO_10		13
TM_PIO_3		8	TM_PIO_11		14

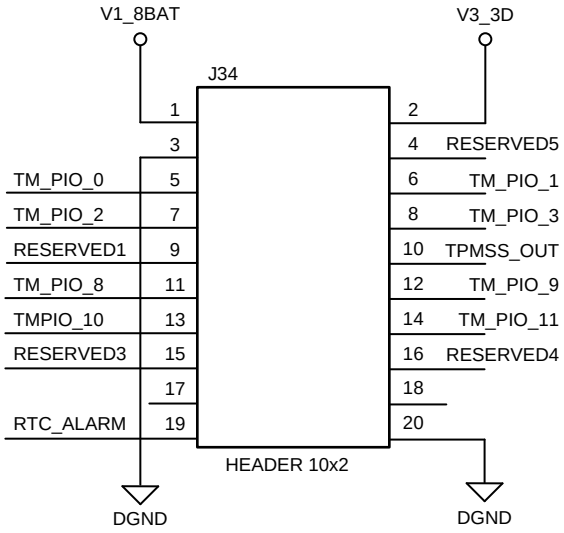


図 16. Wire Mesh Header

Board Connections

- Use J34 and J88 headers to test the wire mesh.
- Make connection should be made according to the pin connections mentioned in 図 16.

表 2. Wire Mesh Pin Configuration

PIO	PIN CONFIGURATION
PIO_0	Pin 5 and 11
PIO_1	Pin 6 and 12
PIO_2	Pin 7 and 13
PIO_3	Pin 8 and 14

PIO Combinations

The combinations of the PIOs that can be connected as wire meshes are fixed. The PIOs can be paired as PIO_0 to PIO_8, PIO_1 to PIO_9, and so on to configure wire meshes. First configure the PIOs based on the wire meshes required. The remaining PIOs can be used for open close switches.

For wire mesh configurations, PIO_0 through PIO_5 must be configured as TX and PIO_8 through PIO_13 must be configured as RX.

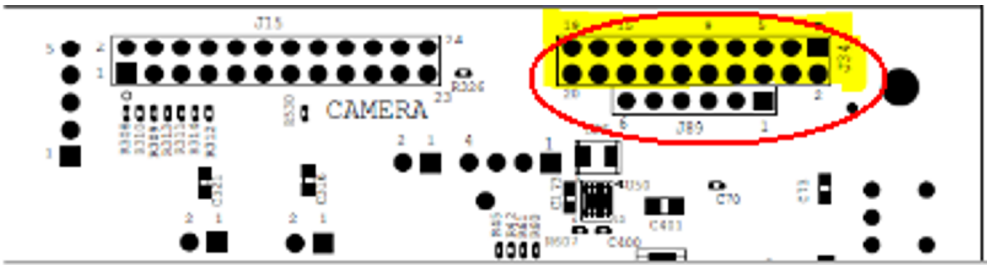


図 17. Wire Mesh Connections for Four PIOs

Hardware Requirements for Testing

- Female-to-female pin connector

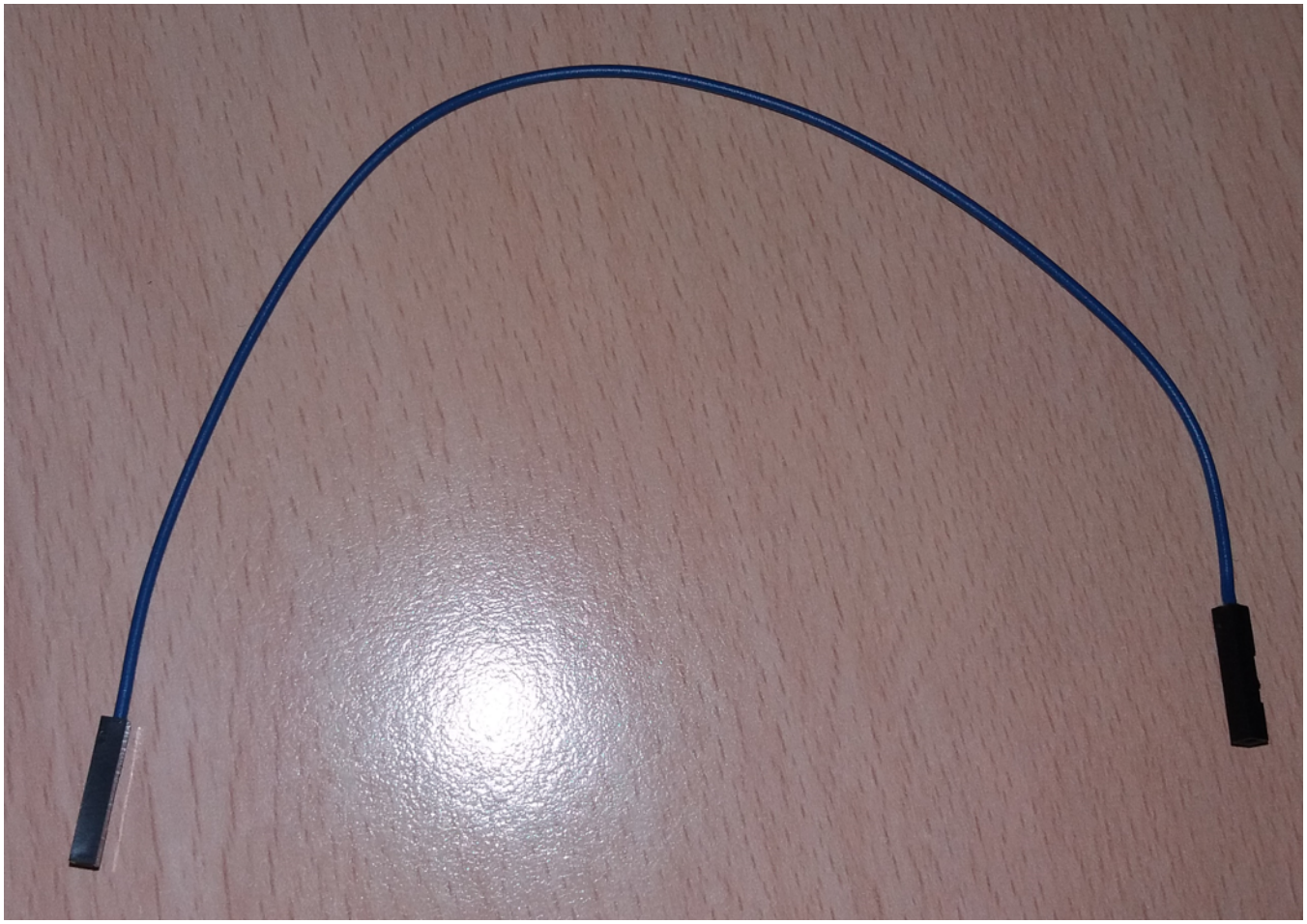


図 18. Pin Connector for Wire Mesh

How to Test Wire Mesh

Currently the wire mesh is tested using U-Boot by halting it during boot-up. The following are instructions and screenshots for testing wire mesh:

1. Halt U-Boot during boot-up by pressing Enter.

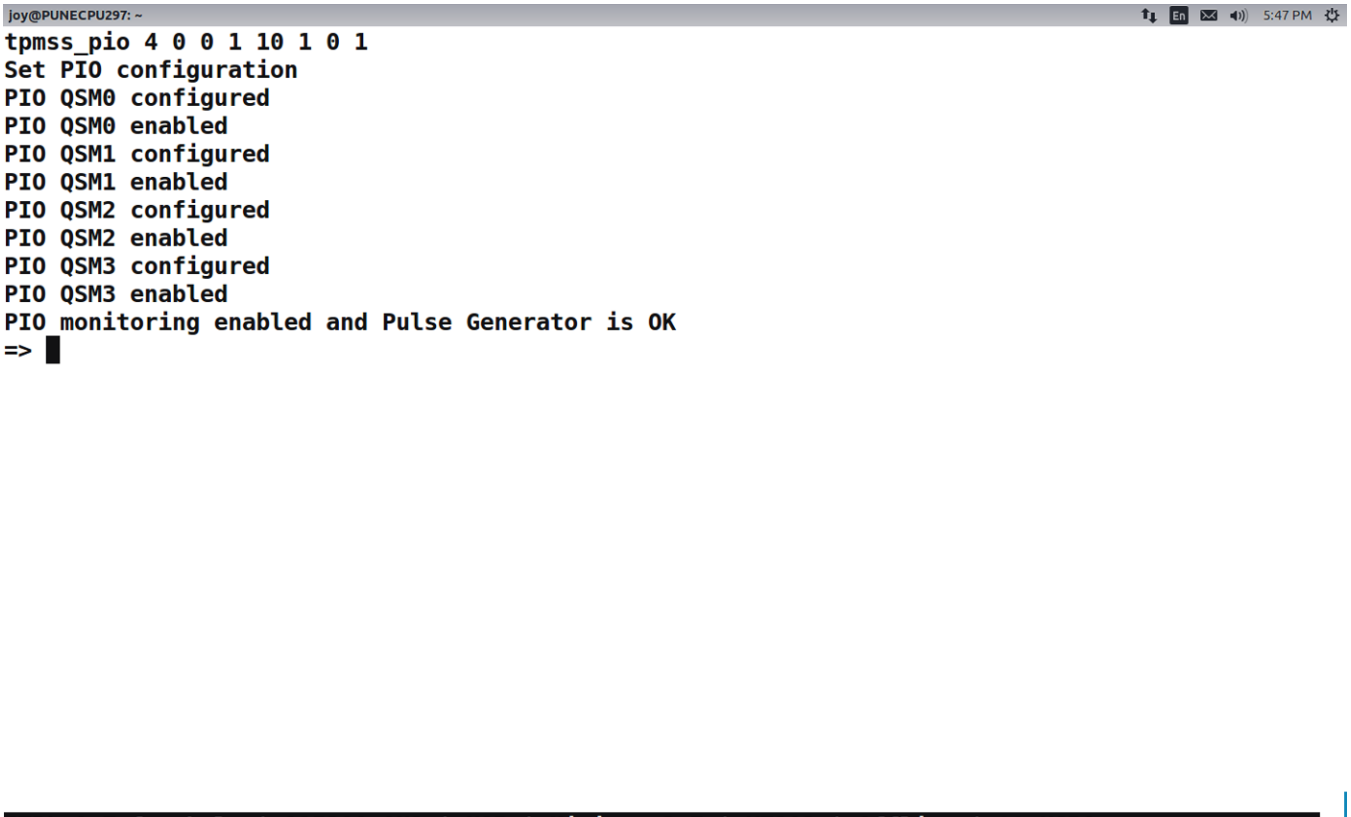


図 19. Configuring Four PIOs on U-Boot Prompt

Command information:

- <n_meshes>—number of wire mesh: 4
- <n_switches>—number of enclosure switches: 0

> **注:** The combinations of the PIOs that can be connected as wire meshes are fixed. The PIOs can be paired as PIO_0 to PIO_8, PIO_1 to PIO_9, and so on. Go on shorting loops starting from pair 0 to the number of pairs selected in this example.

- <irq>—enable IRQ on tamper [reset = 0]: 0
- <bbdmem>—clear BBD memory on tamper [reset=0]: 1
- <thrctr>—Event counter threshold for FREQ QSM [reset = 4]: 10
- <distimer>—disable timer mode [reset = 0]: 1
- <tmrctr>—Timer counter value for FREQ QSM [reset = 0]: 0
- <qsm enable>—Enables FREQ QSM (1 = State Machine enabled, 0 = State Machine disabled): 1

2. Apply the command "tpmss_prolog" to unlock the core, bbd RAM, and some initialization.
3. Initialize the number of PIOs required.

注: For demonstration purposes, four PIOs are used to test.

4. Dump the error log without breaking any loops (and without opening any PIOs).

図 20. TPMSS Log Before Breaking Loop

5. Dump the error after breaking any loops.

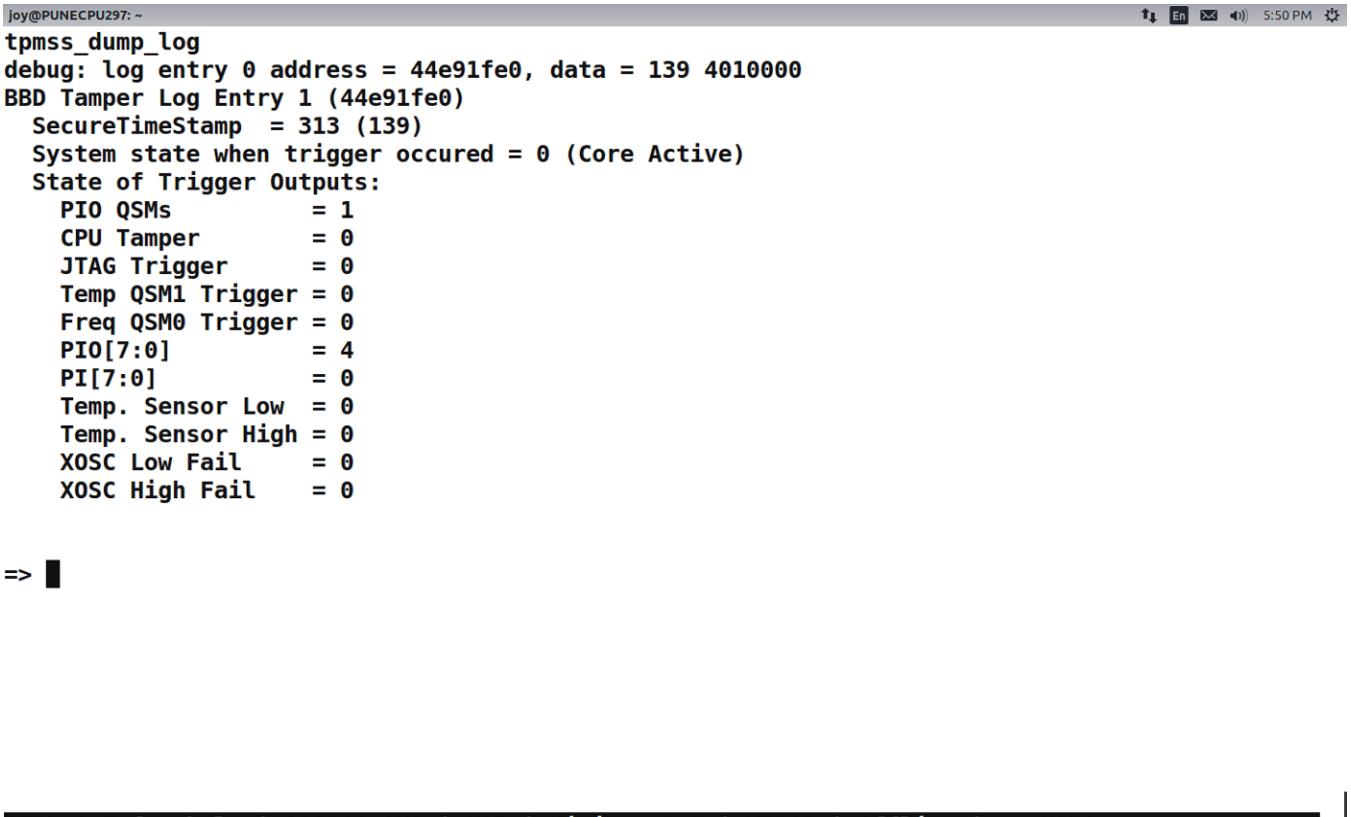


図 21. TPMSS Log After Breaking Loop

注: In this example, the loop breaks by removing the PIO_2 connector (pin 7 or 13). Command: tpmss_dump_log

The output value is the bit position, which provides the PIO number.

If the following combinations are removed:

- PIO_0 (pin 5 and 11): Error output for PIO [7:0] = 1
- PIO_1 (pin 6 and 12): Error output for PIO [7:0] = 2
- PIO_2 (pin 7 and 13): Error output for PIO [7:0] = 4
- PIO_3 (pin 8 and 14): Error output for PIO [7:0] = 8

注: In this example, the value is 4, which is the PIO_2 connector.

4 Design Files

4.1 Schematics

To download the schematics, see the design files at TIDEP-0093.

4.2 Bill of Materials

To download the bill of materials (BOM), see the design files at TIDEP-0093.

4.3 PCB Layout Recommendations

4.3.1 Layout Prints

To download the layer plots, see the design files at TIDEP-0093.

4.4 Altium Project

To download the Altium project files, see the design files at TIDEP-0093.

4.5 Gerber Files

To download the Gerber files, see the design files at TIDEP-0093.

4.6 Assembly Drawings

To download the assembly drawings, see the design files at TIDEP-0093.

5 Software Files

The AM438x EPOS SDK is a restricted-access software package that requires business approval and special NDA with TI before access is provided through the TI secure delivery portal (mySecure Software). Contact a local TI representative for details. Request access using the following link: https://www.ti.com/licreg/docs/swlicexportcontrol.tsp?form_id=250333&prod_no=AM438X_RESTRICTED_SW&ref_url=sitara

The AM438x EPOS SDK package contains a software user's guide and additional documentation for setting up and running the demo test applications.

6 Related Documentation

1. TI E2E Community, *Texas Instruments Security Private E2E*
2. Texas Instruments, *AM438x EPOS EVM Hardware's User's Guide*, User's Guide (SPRUIF8)

6.1 商標

7 Terminology

EPOS— Electronic point of sale

PCI-PTS— Payment card industry pin transaction security

8 About the Authors

AMRIT MUNDRA is a part of the system team in the Catalog Processors BU. He has been with TI for more than 14 years and has worked on multiple IPs and SoCs. He is the security architect for Keystone3 and security lead for Catalog BU. Amrit also is System lead for EPOS EE initiative in BU. Amrit earned his master of science in electrical engineering (MSEE) from SMU, Dallas, TX.

CARLOS BETANCOURT is a product marketing engineer at Texas Instruments, where he is responsible for marketing Sitara processors. Carlos earned his bachelor and master of science in electrical engineering degrees from the University of Texas at El Paso in 1997 and 1999, respectively.

JAMES DOUBLESIN is a member of the hardware applications team in the Catalog Processors Business Unit. He has worked at TI for more than 24 years and has been involved with many different ARM-based embedded processors in the Sitara product line. James earned his BS in electrical engineering from Southern Methodist University and MS in electrical engineering from University of Texas at Arlington.

YOGESH SIRASWAR is a software project lead for Processor SDK EPOS in the Catalog Processors Business Unit. He has worked at TI for more than 15 years and delivered various software on many different DSP and ARM-based embedded processors. Yogesh has earned his BS in electronic & communication engineering from Maulana Azad National Institute of Technology, Bhopal.

TIの設計情報およびリソースに関する重要な注意事項

Texas Instruments Incorporated ("TI")の技術、アプリケーションその他設計に関する助言、サービスまたは情報は、TI製品を組み込んだアプリケーションを開発する設計者に役立つことを目的として提供するものです。これにはリファレンス設計や、評価モジュールに関係する資料が含まれますが、これらに限られません。以下、これらを総称して「TIリソース」と呼びます。いかなる方法であっても、TIリソースのいずれかをダウンロード、アクセス、または使用した場合、お客様(個人、または会社を代表している場合にはお客様の会社)は、これらのリソースをここに記載された目的にのみ使用し、この注意事項の条項に従うことに合意したものとします。

TIによるTIリソースの提供は、TI製品に対する該当の発行済み保証事項または免責事項を拡張またはいかなる形でも変更するものではなく、これらのTIリソースを提供することによって、TIにはいかなる追加義務も責任も発生しないものとします。TIは、自社のTIリソースに訂正、拡張、改良、およびその他の変更を加える権利を留保します。

お客様は、自らのアプリケーションの設計において、ご自身が独自に分析、評価、判断を行う責任がお客様にあり、お客様のアプリケーション(および、お客様のアプリケーションに使用されるすべてのTI製品)の安全性、および該当するすべての規制、法、その他適用される要件への遵守を保証するすべての責任をお客様のみが負うことを理解し、合意するものとします。お客様は、自身のアプリケーションに関して、(1) 故障による危険な結果を予測し、(2) 障害とその結果を監視し、および、(3) 損害を引き起こす障害の可能性を減らし、適切な対策を行う目的での、安全策を開発し実装するために必要な、すべての技術を保持していることを表明するものとします。お客様は、TI製品を含むアプリケーションを使用または配布する前に、それらのアプリケーション、およびアプリケーションに使用されているTI製品の機能性を完全にテストすることに合意するものとします。TIは、特定のTIリソース用に発行されたドキュメントで明示的に記載されているもの以外のテストを実行していません。

お客様は、個別のTIリソースにつき、当該TIリソースに記載されているTI製品を含むアプリケーションの開発に関連する目的でのみ、使用、コピー、変更することが許可されています。明示的または黙示的を問わず、禁反言の法理その他どのような理由でも、他のTIの知的所有権に対するその他のライセンスは付与されません。また、TIまたは他のいかなる第三者のテクノロジまたは知的所有権についても、いかなるライセンスも付与されるものではありません。付与されないものには、TI製品またはサービスが使用される組み合わせ、機械、プロセスに関連する特許権、著作権、回路配置利用権、その他の知的所有権が含まれますが、これらに限られません。第三者の製品やサービスに関する、またはそれらを参照する情報は、そのような製品またはサービスを利用するライセンスを構成するものではなく、それらに対する保証または推奨を意味するものでもありません。TIリソースを使用するため、第三者の特許または他の知的所有権に基づく第三者からのライセンス、あるいはTIの特許または他の知的所有権に基づくTIからのライセンスが必要な場合があります。

TIのリソースは、それに含まれるあらゆる欠陥も含めて、「現状のまま」提供されます。TIは、TIリソースまたはその仕様に関して、明示的か暗黙的かにかかわらず、他のいかなる保証または表明も行いません。これには、正確性または完全性、権原、続発性の障害に関する保証、および商品性、特定目的への適合性、第三者の知的所有権の非侵害に対する黙示の保証が含まれますが、これらに限られません。

TIは、いかなる苦情に対しても、お客様への弁護または補償を行う義務はなく、行わないものとします。これには、任意の製品の組み合わせに関連する、またはそれらに基づく侵害の請求も含まれますが、これらに限られず、またその事実についてTIリソースまたは他の場所に記載されているか否かを問わないものとします。いかなる場合も、TIリソースまたはその使用に関連して、またはそれらにより発生した、実際的、直接的、特別、付随的、間接的、懲罰的、偶発的、または、結果的な損害について、そのような損害の可能性についてTIが知らされていたかどうかにかかわらず、TIは責任を負わないものとします。

お客様は、この注意事項の条件および条項に従わなかったために発生した、いかなる損害、コスト、損失、責任からも、TIおよびその代表者を完全に免責するものとします。

この注意事項はTIリソースに適用されます。特定の種類の資料、TI製品、およびサービスの使用および購入については、追加条項が適用されます。これには、半導体製品(http://www.ti.com/sc/docs/stdterms.htm)、評価モジュール、およびサンプル(http://www.ti.com/sc/docs/sampterms.htm)についてのTIの標準条項が含まれますが、これらに限られません。