TI 参考设计：TIDEP-0093
电子销售终端 (EPOS) 支付终端参考设计

说明

TIDEP-0093 设计利用一款可帮助客户满足 PCI-PTS 和 EMV 要求的处理器，加快推向市场的速度。电子销售终端 (EPOS) 支付终端需要 经认证启动、 篡改检测、 DDR 加密等功能。借助该 AM438x 处理器，开发人员能够设计出符合支付卡行业 (PCI) 认证的系统。AM438x 处理器可提供扩展性，具备各种处理器速度和兼容软件，可满足低端至高端 应用需求，此外还提供充足的连接，其中包括支付终端所需的关键外设（如智能卡和磁卡读卡器）。

资源

TIDEP-0093	设计文件夹
AM438x	产品文件夹
TPS65218	产品文件夹
TCA5013	产品文件夹

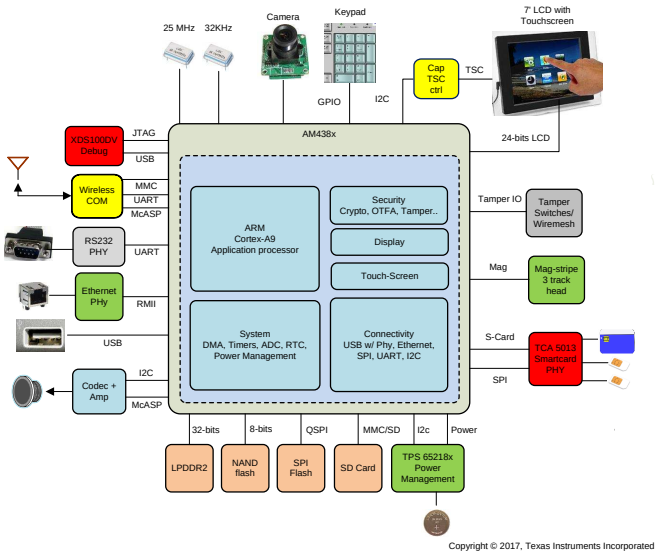
TI E2E™ Community — 咨询我们的 E2E 专家

特性

- 具有集成功能的 TI Sitara™AM438x 处理器 可帮助客户设计销售终端 应用
- 基于 ARM® Cortex®-A9 的处理器具有 300MHz、600MHz 和 1GHz 的速度，以及 3D 图形和 PRU 选项
- 用于 Linux®开发的处理器软件开发套件 (SDK)
- 智能卡和磁卡读卡器以及其他外设，如触摸显示屏、键盘、USB、以太网等
- 包括 TI TPS65218 电源管理 IC 和 TCA5013 智能卡 PHY 器件

应用

- 销售、支付和零钱兑换机
- 手持式和固定式 EFT 终端
- EPOS、ECR 和钱柜
- 燃油加油机
- EPOS 打印机
- ATM



该 TI 参考设计末尾的重要声明表述了授权使用、知识产权问题和其他重要的免责声明和信息。

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. 图 1 shows the Sitara AM438x.

图 **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. 图 2 shows the TPS65218x.

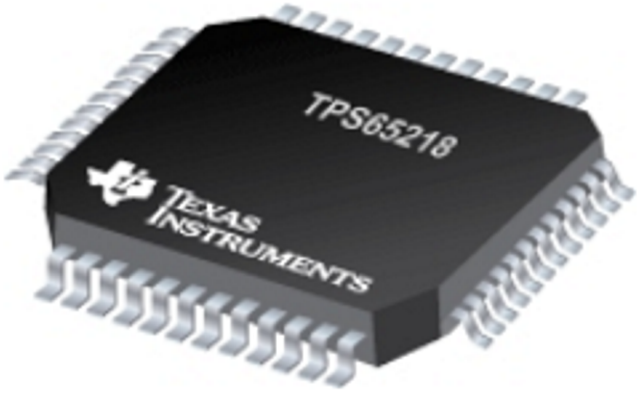


图 **2. TPS65218x**

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. 图 3 shows the TCA5013.

图 **3. TCA5013**

2 System Overview

2.1 Block Diagram

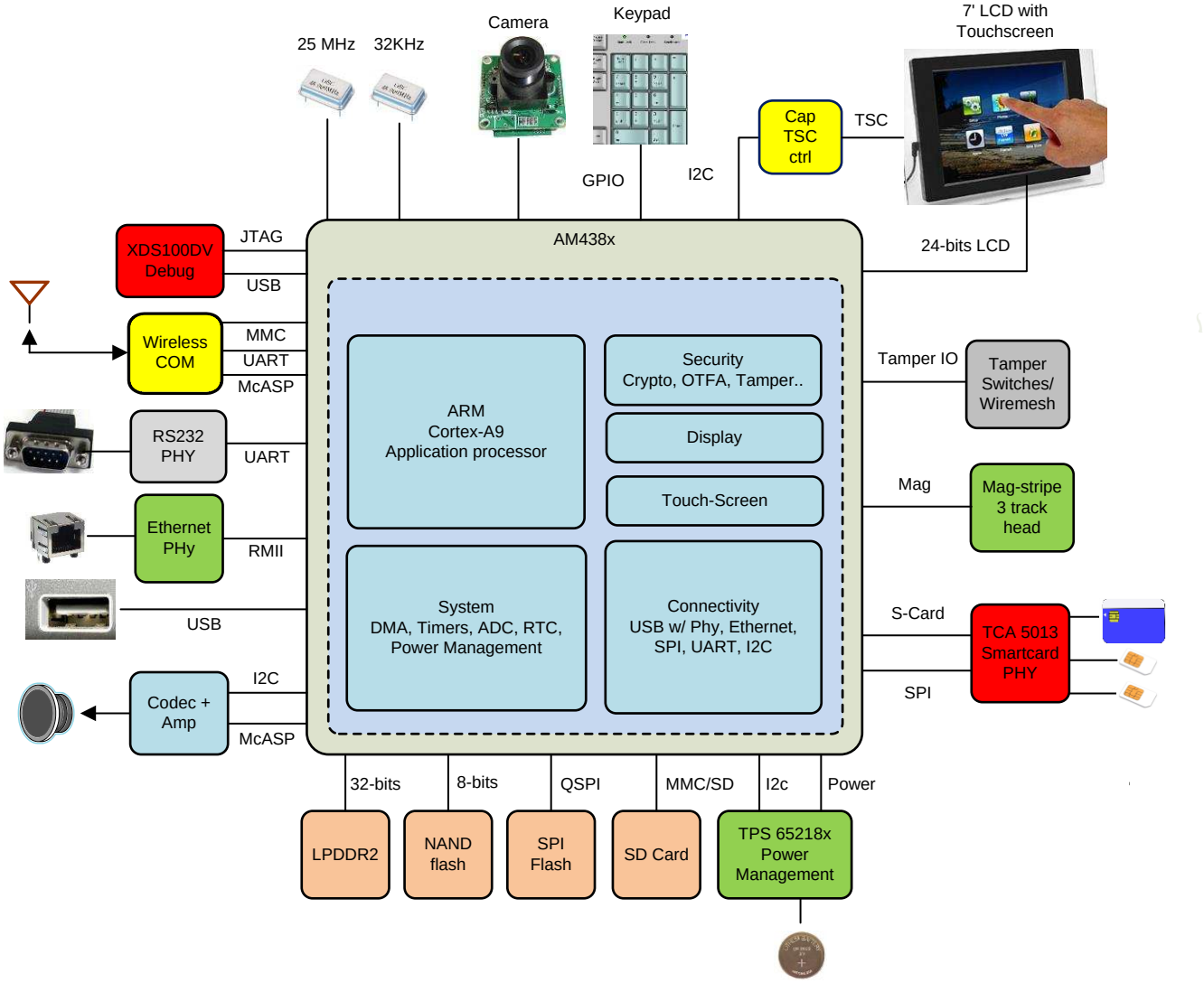


图 4. EPOS EVM System Block Diagram

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.

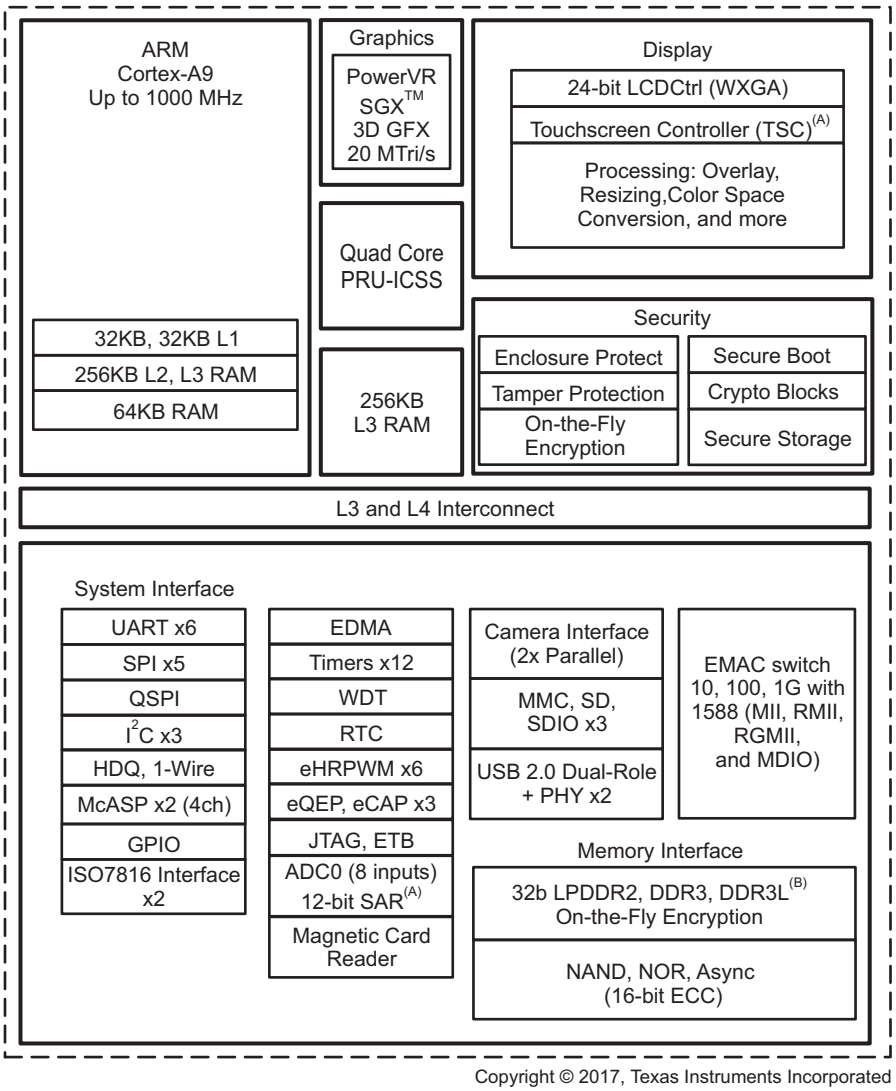


图 **5. AM438x Functional Block Diagram**

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.

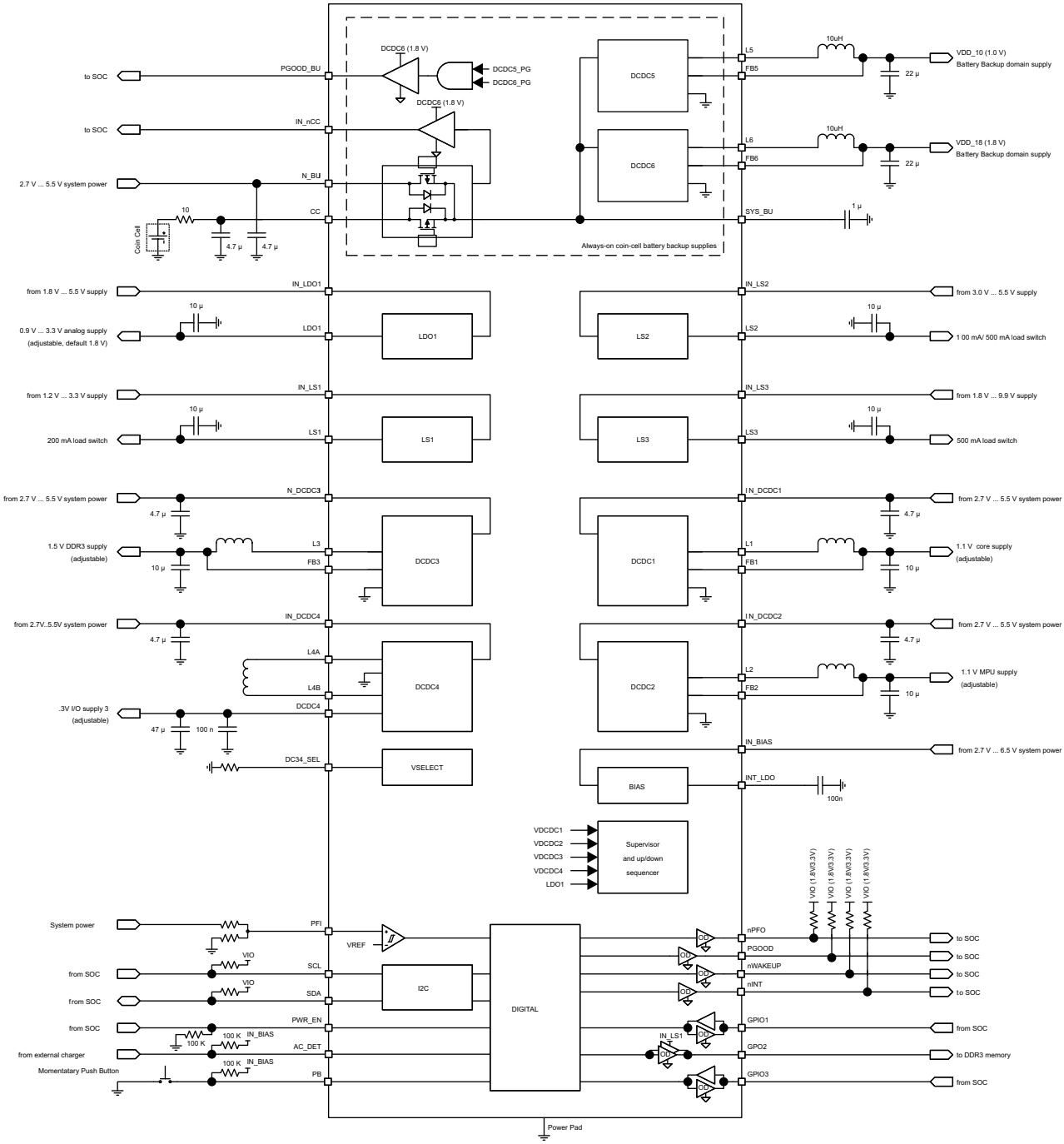


图 **6. TPS65218x Functional Block Diagram**

The I^2C 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 I^2C. 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 I^2C 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 I^2C.

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.

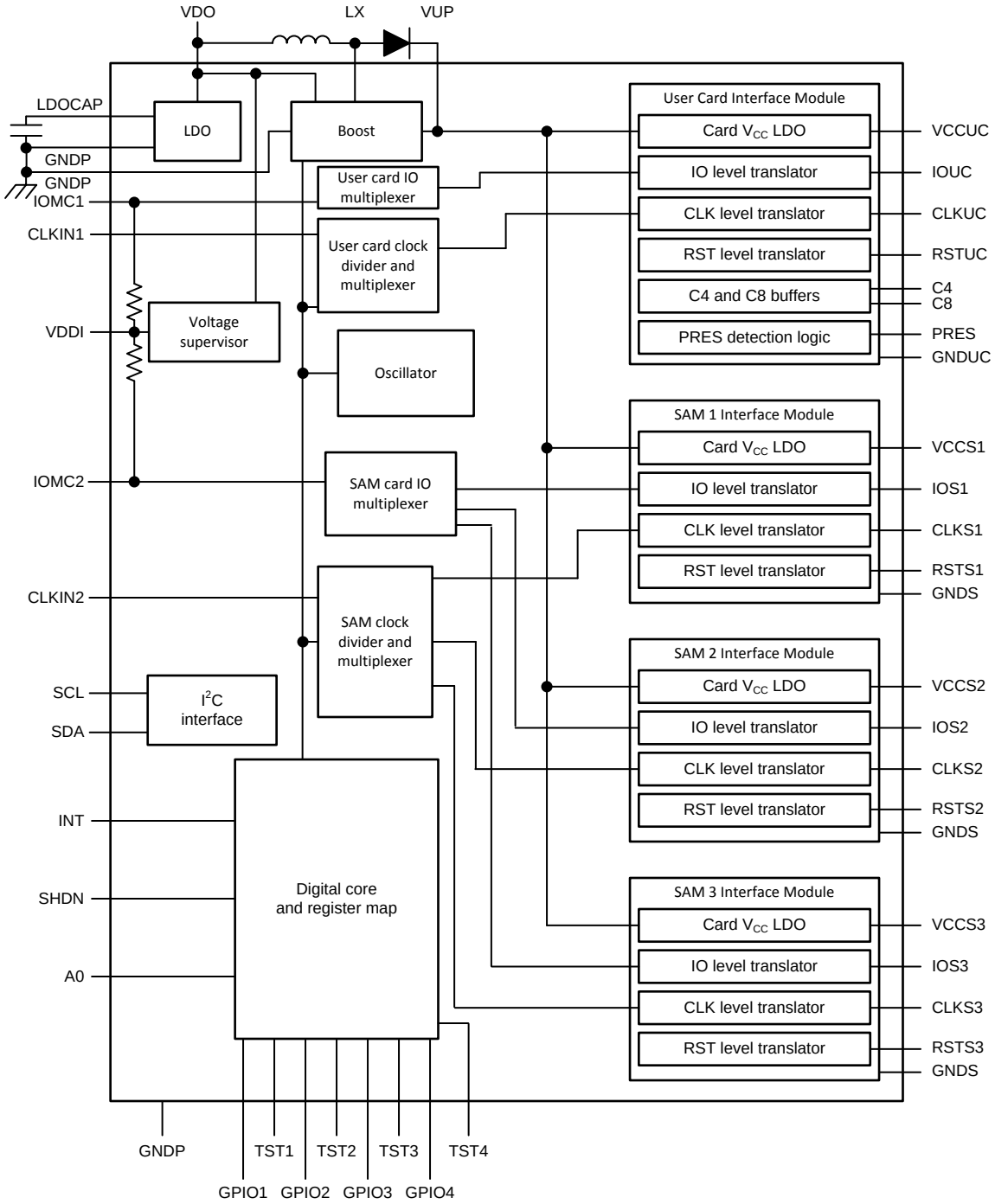


图 7. TCA5013 Functional Block Diagram

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 节 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.

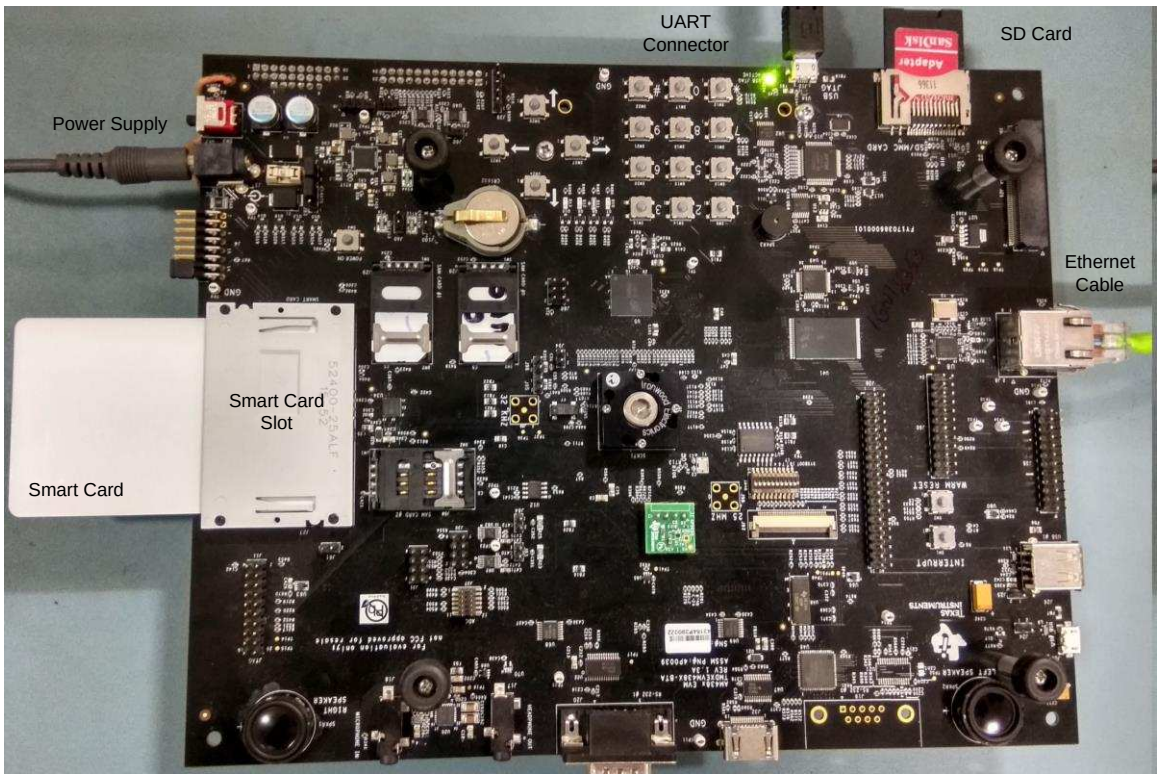


图 **8. AM438x EVM Setup**

3.2.2 Test Results

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

图 **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 图 10).

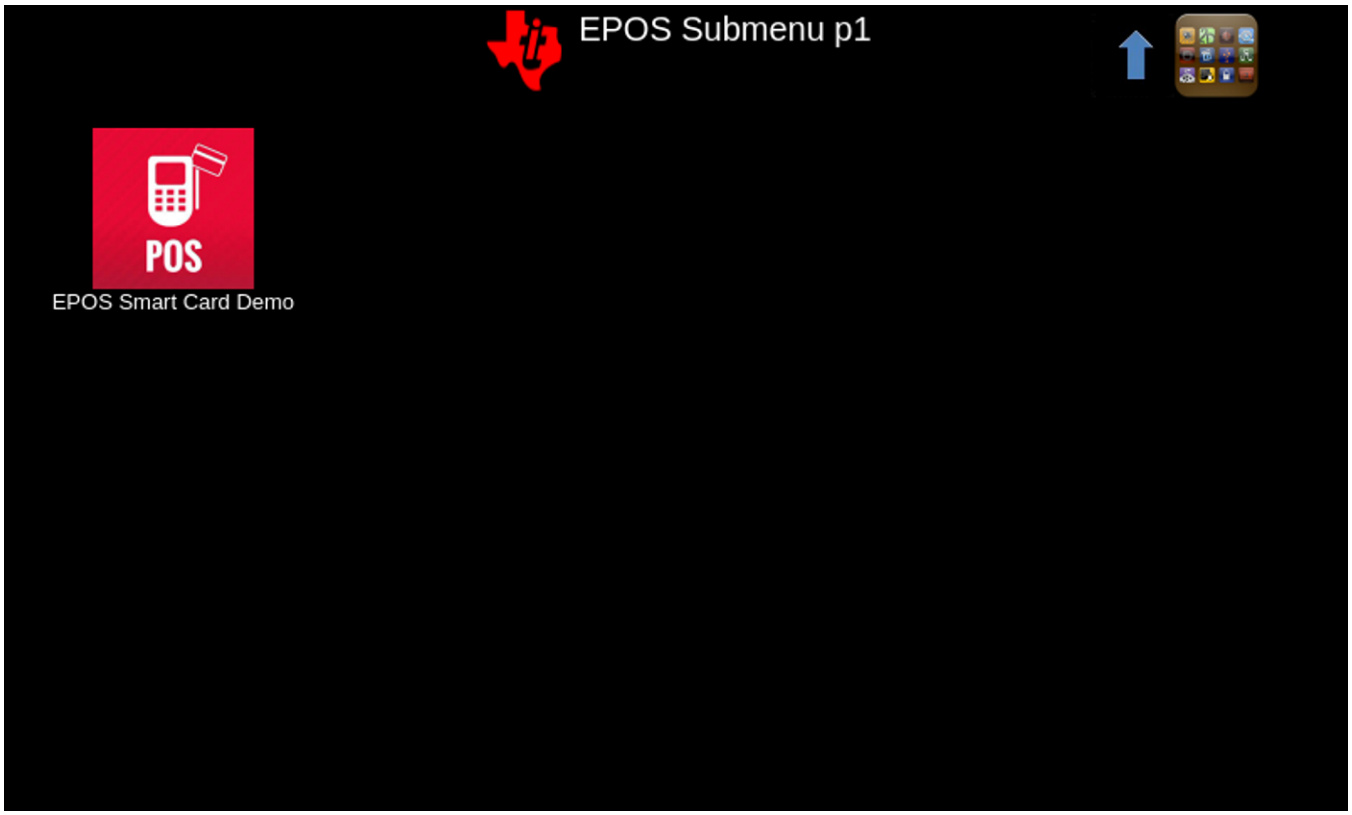


图 10. EPOS Submenu to Launch EPOS Smart Card Demo

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

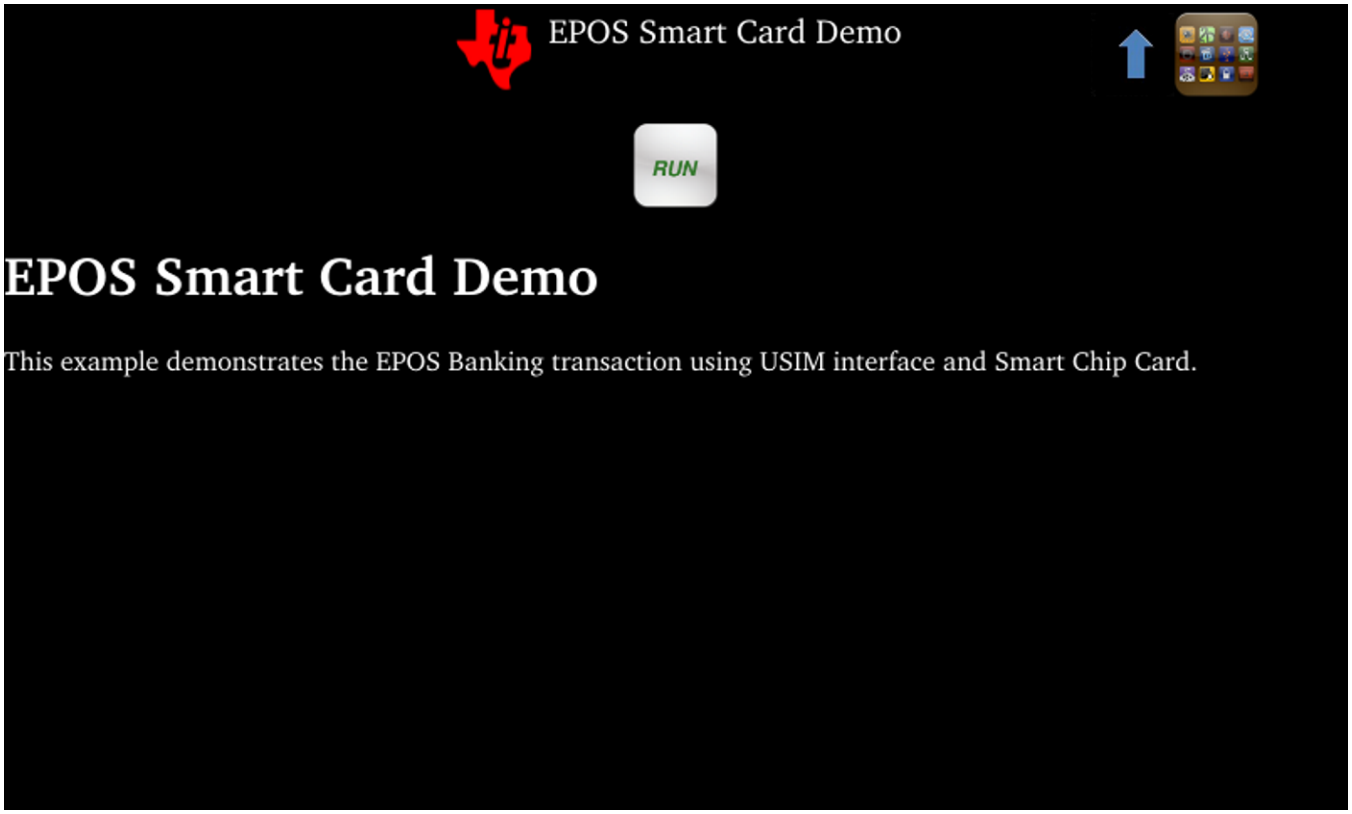


图 **11. EPOS Smart Card Demo Home Screen**

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

图 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 图 13.

图 **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.

图 **14. PIN Authentication Login**

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

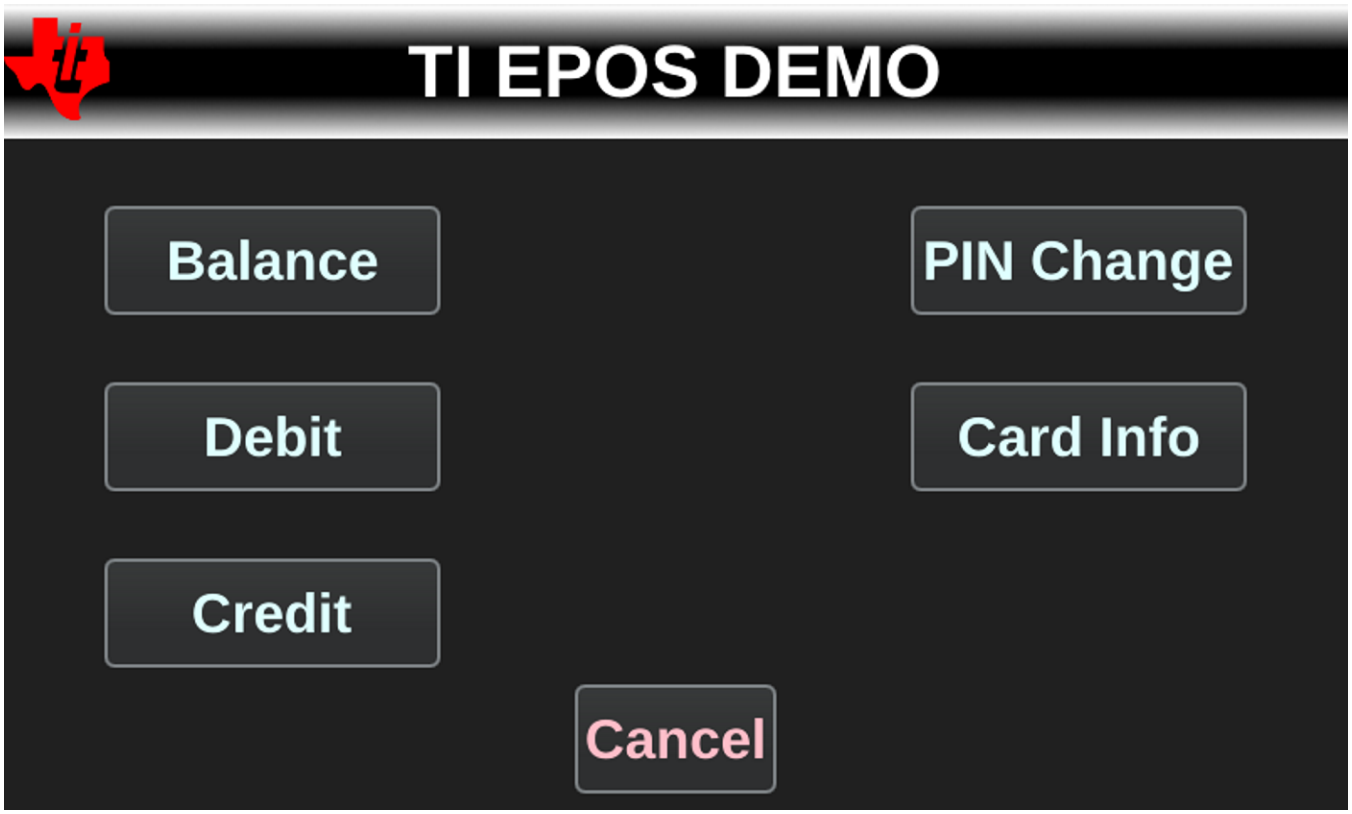


图 **15. PIN Authentication Successful**

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

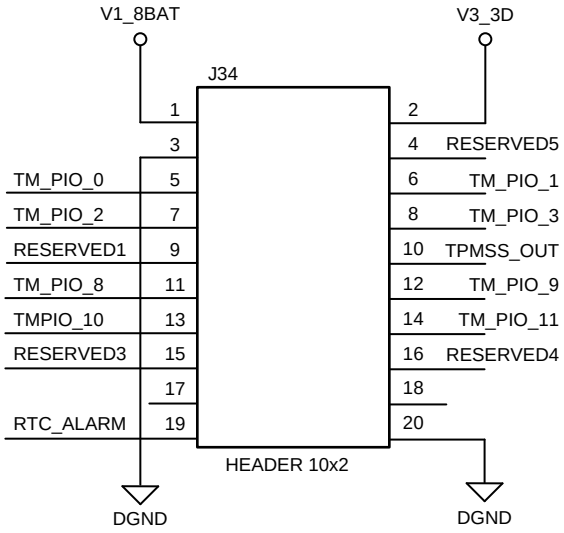


图 **16. Wire Mesh Header**

Board Connections

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

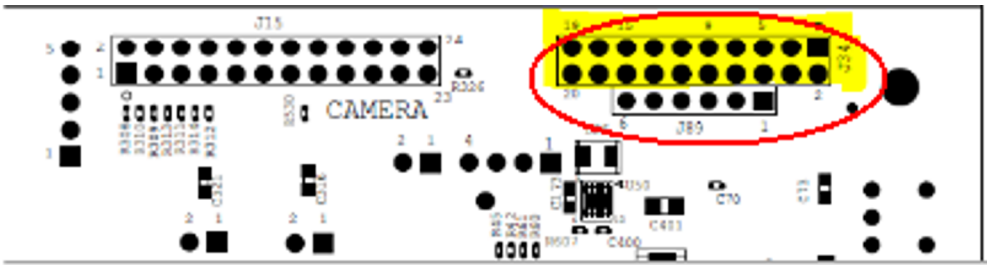


图 **17. Wire Mesh Connections for Four PIOs**

Hardware Requirements for Testing

- Female-to-female pin connector

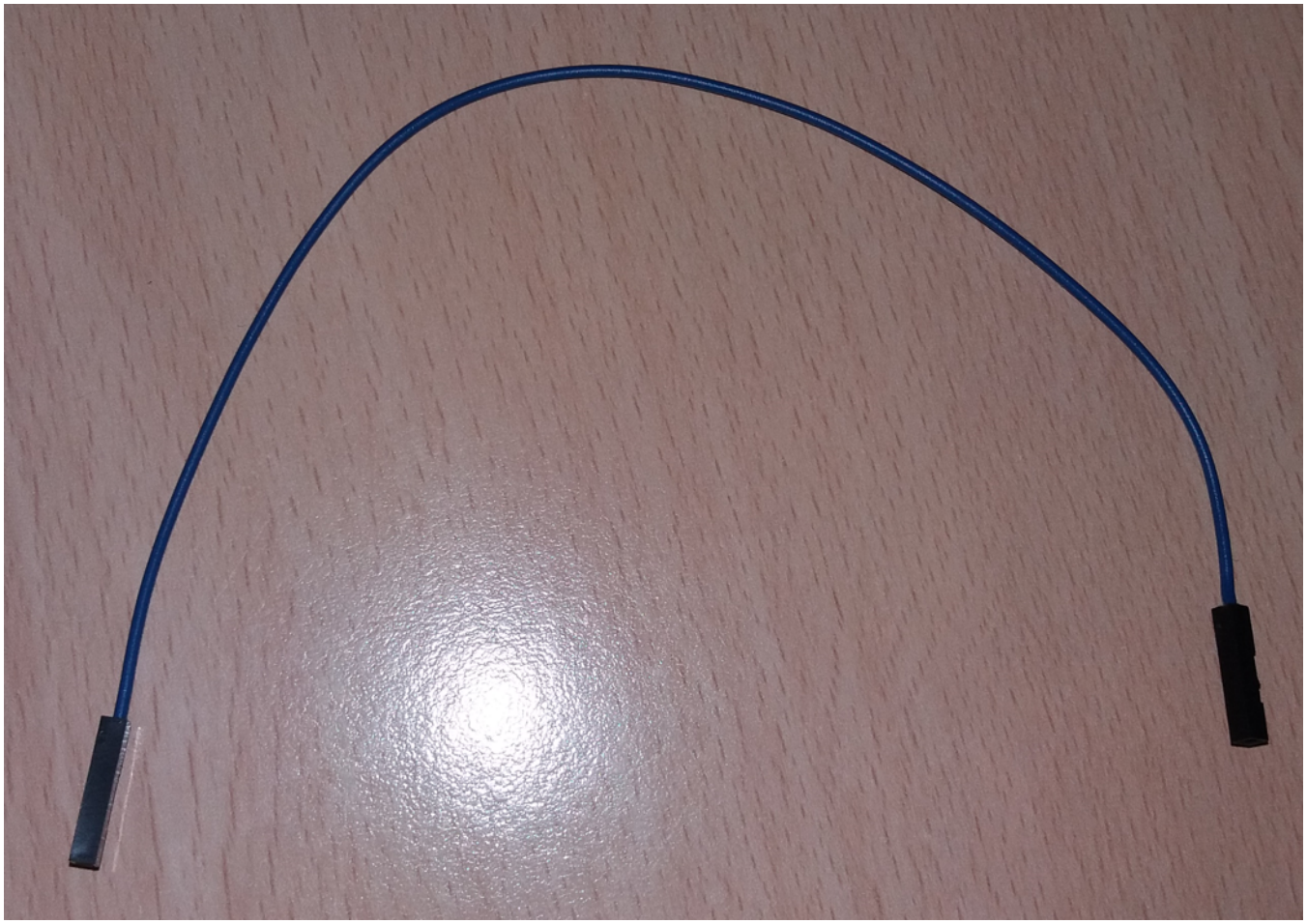


图 **18. Pin Connector for Wire Mesh**

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.

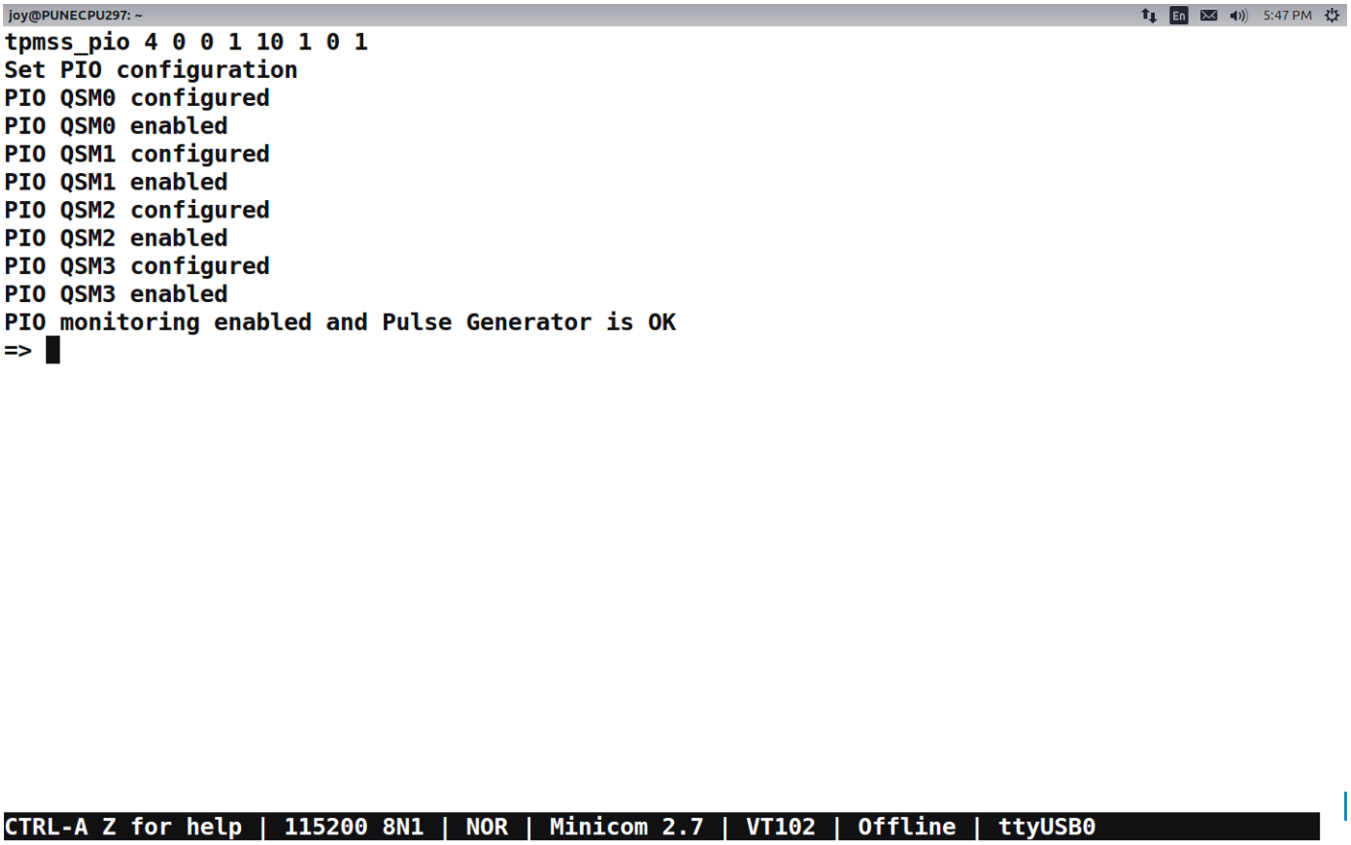


图 **19. Configuring Four PIOs on U-Boot Prompt**

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).

图 **20. TPMSS Log Before Breaking Loop**

5. Dump the error after breaking any loops.

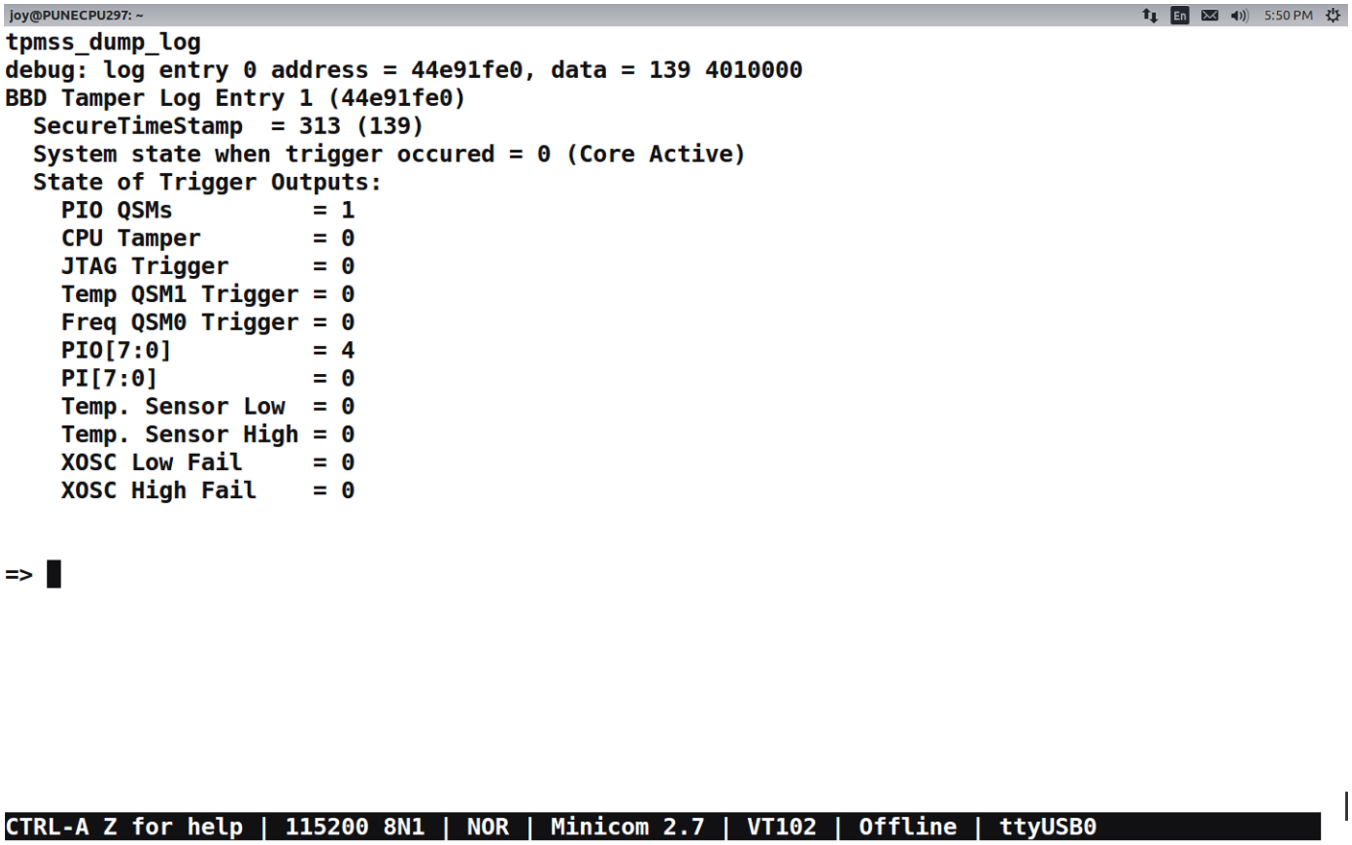


图 **21. TPMSS Log After Breaking Loop**

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 商标

Sitara is a trademark of Texas Instruments, Inc..
基于 ARM, Cortex, TrustZone are registered trademarks of ARM Limited.
PowerVR SGX is a trademark of Imagination Technologies Limited.
Linux is a registered trademark of The Linux Foundation.
All other trademarks are the property of their respective owners.

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.

有关 TI 设计信息和资源的重要通知

德州仪器 (TI) 公司提供的技术、应用或其他设计建议、服务或信息，包括但不限于与评估模块有关的参考设计和材料（总称“TI 资源”），旨在帮助设计人员开发整合了 TI 产品的 应用； 如果您（个人，或如果是代表贵公司，则为贵公司）以任何方式下载、访问或使用了任何特定的 TI 资源，即表示贵方同意仅为该等目标，按照本通知的条款进行使用。

TI 所提供的 TI 资源，并未扩大或以其他方式修改 TI 对 TI 产品的公开适用的质保及质保免责声明；也未导致 TI 承担任何额外的义务或责任。TI 有权对其 TI 资源进行纠正、增强、改进和其他修改。

您理解并同意，在设计应用时应自行实施独立的分析、评价和 判断， 且应全权负责并确保 应用的安全性， 以及您的 应用 （包括应用中使用的所有 TI 产品）） 应符合所有适用的法律法规及其他相关要求。你就您的 应用声明，您具备制订和实施下列保障措施所需的一切必要专业知识，能够 (1) 预见故障的危险后果，(2) 监视故障及其后果，以及 (3) 降低可能导致危险的故障几率并采取适当措施。您同意，在使用或分发包含 TI 产品的任何 应用前， 您将彻底测试该等 应用 和该等应用所用 TI 产品的 功能。除特定 TI 资源的公开文档中明确列出的测试外，TI 未进行任何其他测试。

您只有在为开发包含该等 TI 资源所列 TI 产品的 应用时， 才被授权使用、复制和修改任何相关单项 TI 资源。但并未依据禁止反言原则或其他法理授予您任何TI知识产权的任何其他明示或默示的许可，也未授予您 TI 或第三方的任何技术或知识产权的许可，该等产权包括但不限于任何专利权、版权、屏蔽作品权或与使用TI产品或服务的任何整合、机器制作、流程相关的其他知识产权。涉及或参考了第三方产品或服务的信息不构成使用此类产品或服务的许可或与其相关的保证或认可。使用 TI 资源可能需要您向第三方获得对该等第三方专利或其他知识产权的许可。

TI 资源系“按原样”提供。TI 兹免除对 TI 资源及其使用作出所有其他明确或默认的保证或陈述，包括但不限于对准确性或完整性、产权保证、无屡发故障保证，以及适销性、适合特定用途和不侵犯任何第三方知识产权的任何默认保证。

TI 不负责任何申索，包括但不限于因组合产品所致或与之有关的申索，也不为您辩护或赔偿，即使该等产品组合已列于 TI 资源或其他地方。对因 TI 资源或其使用引起或与之有关的任何实际的、直接的、特殊的、附带的、间接的、惩罚性的、偶发的、从属或惩戒性损害赔偿，不管 TI 是否获悉可能会产生上述损害赔偿，TI 概不负责。

您同意向 TI 及其代表全额赔偿因您不遵守本通知条款和条件而引起的任何损害、费用、损失和/或责任。

本通知适用于 TI 资源。另有其他条款适用于某些类型的材料、TI 产品和服务的使用和采购。这些条款包括但不限于适用于 TI 的半导体产品 (http://www.ti.com/sc/docs/stdterms.htm)、评估模块和样品 (http://www.ti.com/sc/docs/sampterms.htm) 的标准条款。

邮寄地址：上海市浦东新区世纪大道 1568 号中建大厦 32 楼，邮政编码：200122