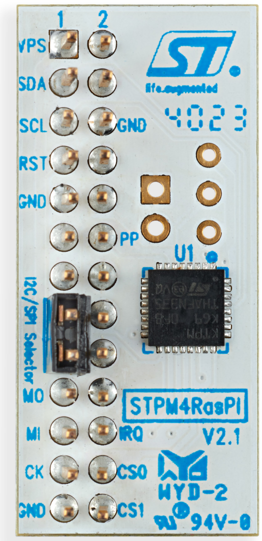
STPM4RasPIV21

Data brief

Evaluation board for STSAFE-TPM ST33KTPM products



Features

- Evaluation board for all STSAFE-TPM devices (ST33KTPM2X for the consumer market and ST33KTPM2I for the industrial market)
- 26-pin female connector to plug on Raspberry Pi® or STM32MPx-DK
- *I²C* or *SPI* configurable interface
- *TPM* reset button to reset the *TPM* device without platform restart
- 26-pin male connector to ease probing and plug the same or another extension board
- Designed to solder an I2C/SPI selector button

Description

The STPM4RasPIV21 is an extension board to connect the ST33KTPM products to the Raspberry Pi® and STM32 microprocessor development kits such as STM32MP157F-DK2, or STM32MP135F-DK. The board is designed for product evaluation, use case development and integration activities. The board is shipped with one trusted platform module soldered. For *TPM* product availability, refer to ordering information section.

Product status link
STPM4RasPIV21

1 STPM4RasPIV21 main features

This section details the main features of STPM4RasPIV21, the extension board connecting the STSAFE-TPM products to the Raspberry Pi® device, STM32MP157F-DK2 and STM32MP135F-DK.

1.1 STPM4RasPIV21 introduction

The STPM4RasPIV21 is a daughter board version 2.1 developed for STSAFE-TPM ST33KTPM device evaluation purposes.

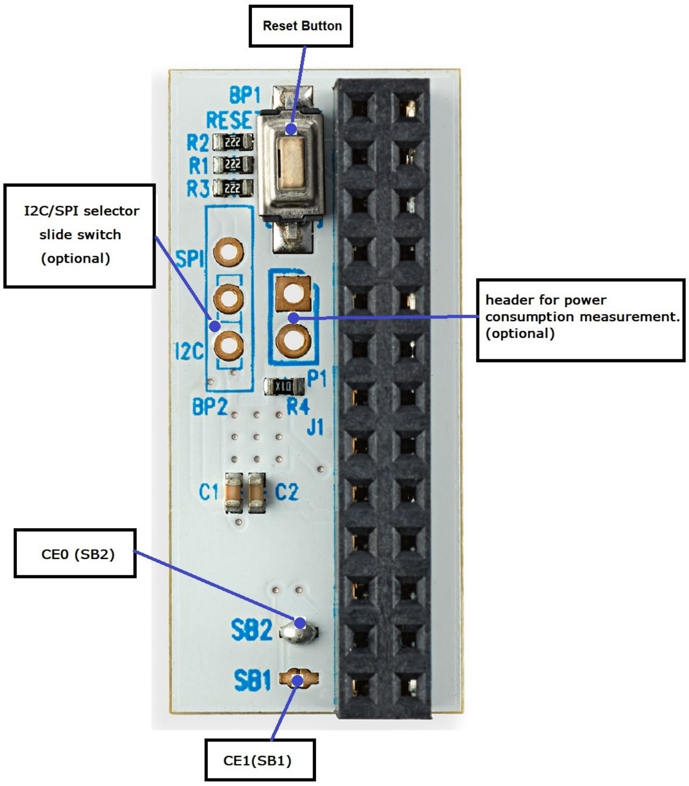
The STPM4RasPIV21 keeps all the legacy functionalities:

- Header for power consumption.
- Crossing pin to probe or to add a new extension board.

The STPM4RasPIV21 brings new features:

- TPM reset button
- I2C/SPI selector
- *SPI* chip selection configuration
- Signals marking on *PCB*

Figure 1. STPM4RasPIV21


Reset Button
I2C/SPI selector slide switch (optional)
header for power consumption measurement. (optional)
CE0 (SB2)
CE1(SB1)
BP1
RESET
R2
R1
R3
SPI
I2C
P1
BP2
R4
J1
C1
C2
SB2
SB1

1.2 Raspberry *SPI* / *I²C* connectivity by *GPIO*

The ST33KTPM2X and ST33KTPM2XI2C products use the following signals:

- MOSI (pin 19)
- MISO (pin 21)
- SCLK (pin 23)
- CE0 (pin 24)
- CE1 (pin 26)
- VCC (pin 1 and 17)
- GND (pin 6, 9, 14, 20 and 25)
- RST (pin 7)
- PIRQ (pin 22)
- PP (pin 12)
- GPI_I2C_SELECT (pin 15)
- SDA (pin 3)
- SCL (pin 5)

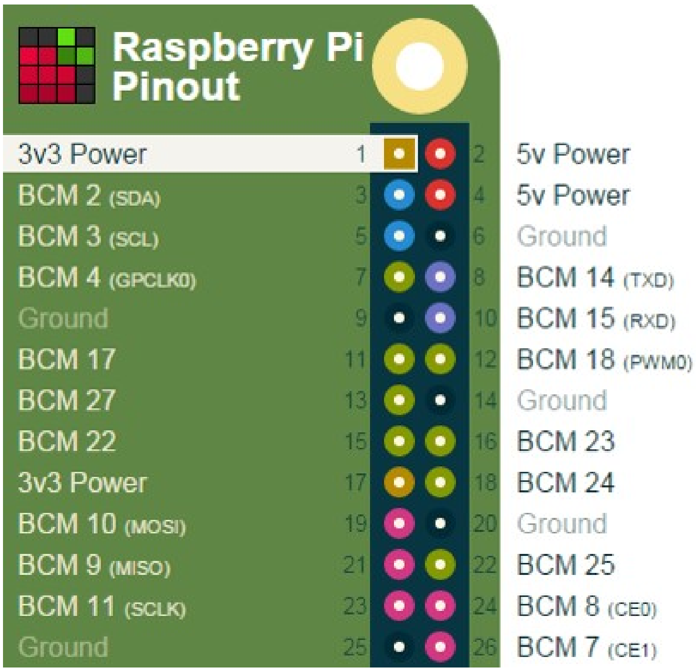


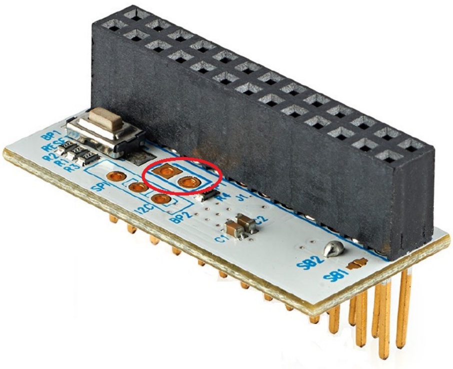
Figure 2. Raspberry Pi *GPIO*

Note: *The STPM4RasPIV21 features a GPIO pin extension reserved for probing or connecting another extension board.*

1.3 TPM power consumption

The P1 pin header can be soldered to plug a multimeter over a 10 Ω resistor (R4) to measure the TPM power consumption.

Figure 3. P1 header location



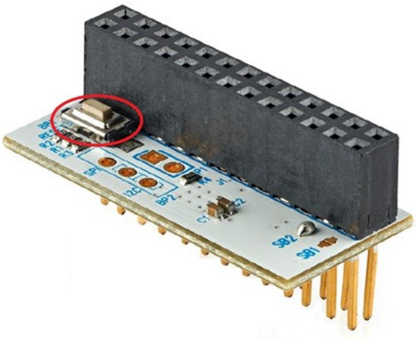
1.4 TPM reset button

The reset button is soldered by default at the bottom of the STPM4RasPIV21.

This button only restarts the TPM device and performs the TPM_Init, as defined in [PTP standard specification].

After reset, users execute a new TPM initialization, such as TPM2_Startup and TPM2_SelfTest.

Figure 4. Reset button



1.5 Bus interface selection

ST33KTPM2X and ST33KTPM2I introduce a new functionality, which allows the exclusive support of both *I²C* and *SPI* bus interfaces on the same chip, with dedicated signals.

The user can select any of the *I²C* or the *SPI* bus interfaces, by using a jumper or a switch slide.

1.5.1 Bus interface selection using a jumper

The user can use a jumper to select the *I²C* or the *SPI* bus interface. When using a jumper, place it as follows:

Table 1. Interface selection by jumper

Interface	Selection method
I²C	GPI_I2C_SELECT (pin 15) with low level
SPI	GPI_I2C_SELECT (pin 15) with high level

Figure 5. Use of the I2C/SPI jumper for the *SPI* interface selection

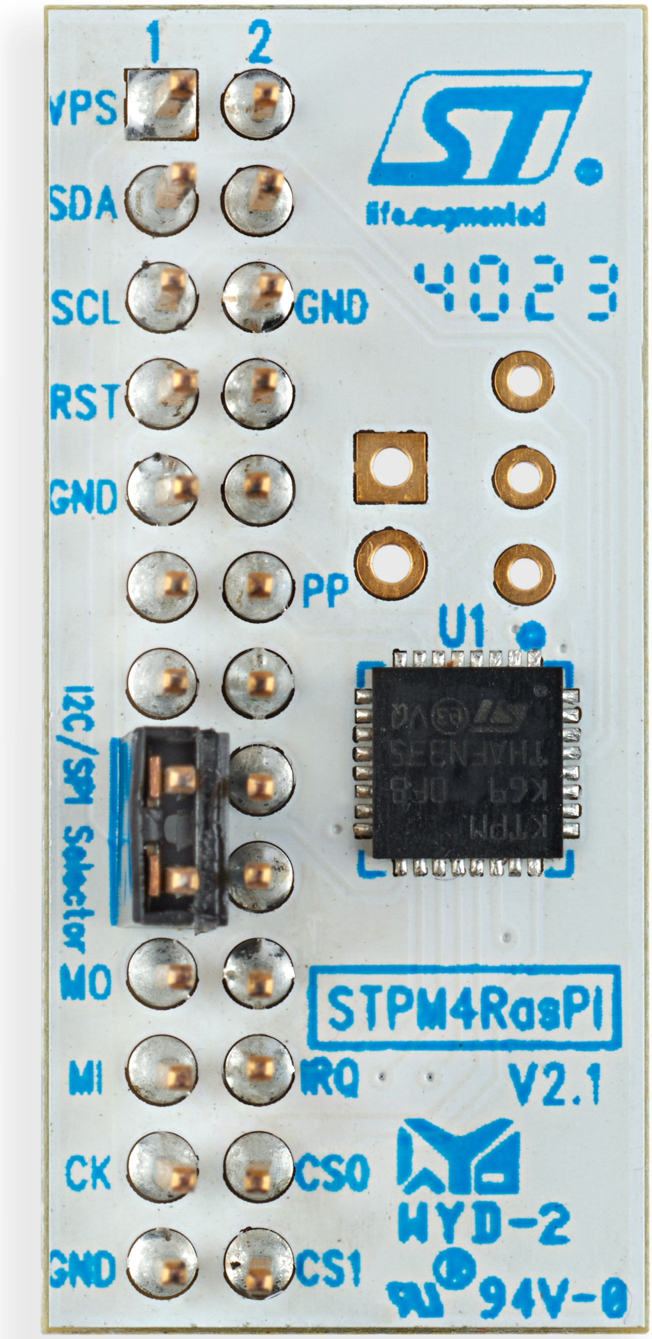
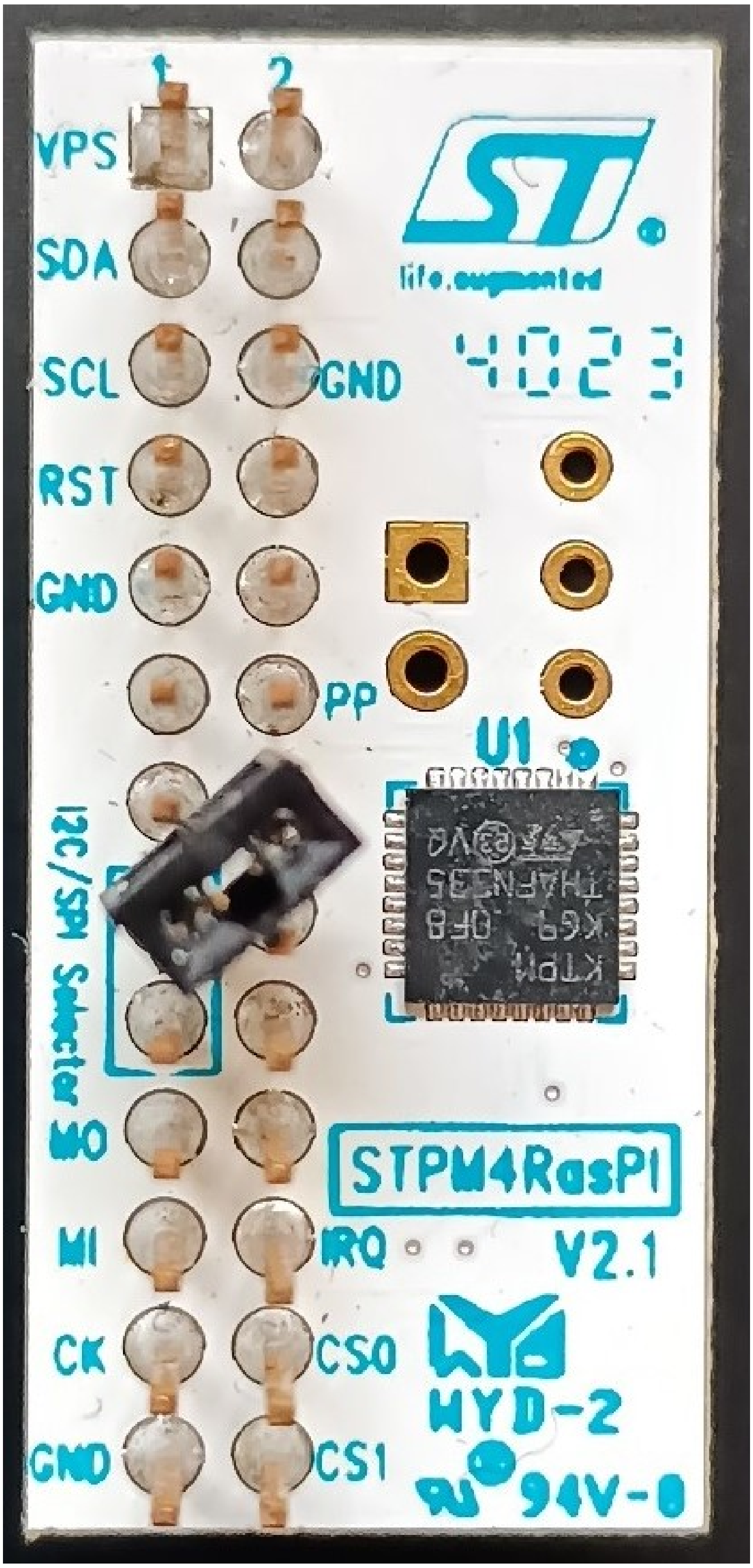


Figure 6. Use of the I2C/SPI jumper for the *I^2C* interface selection



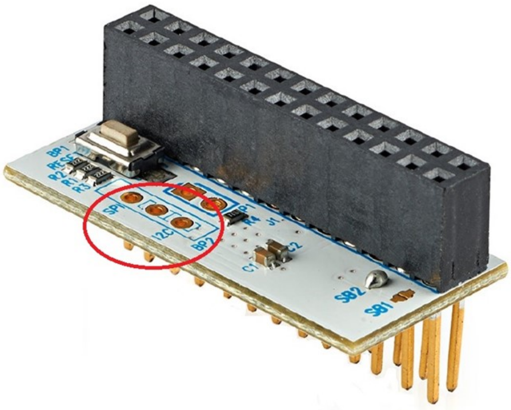
-

1.5.2 Bus interface selection using a switch slide

The switch slide can be soldered at the bottom of the STPM4RasPIV21 to easily select the *TPM* bus interface.

Note: *Using a switch slide is optional.*

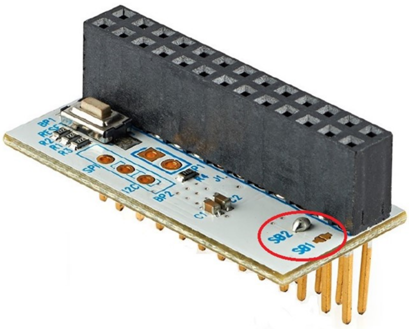
Figure 7. **Use of the switch slide for interface selection**



1.6 Configuration of the SPI chip selection

Raspberry Pi® and STPM32MP1xx can drive up to two *SPI* slaves through CE0 and CE1.
STPM4RasPIV21 is configured by default to CS0 (SB2 soldered).
However, the user can configure CS1 by soldering SB1 and unsoldering SB2.

Figure 8. **SPI chip selection configuration**



1.7 Signal marking on PCB

All signals are marked on the *PCB* to facilitate end-user probing with a logic analyzer.

Figure 9. **Signal marking on *PCB***

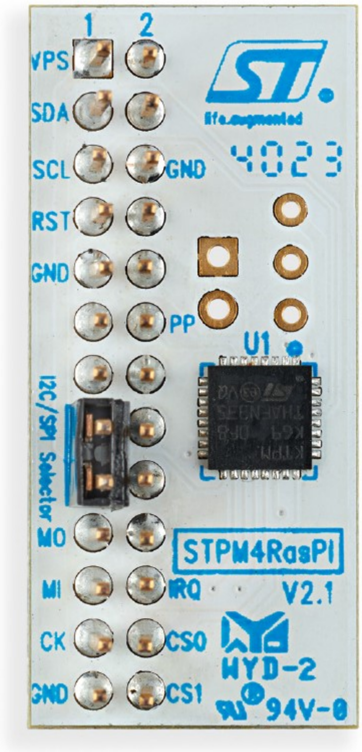


Table 2. **Signal definition**

Signal	Definition
VPS	Power supply at 3.3 V
SDA	Bidirectional *I²C* serial data
SCL	Input *I²C* serial clock
GND	Ground
RST	Reset, active low, used to reinitialize the device
PP	Physical presence (*PP*), active high, internal pull-down
I2C/SPI selector	GPIO15 to connect VPS (*SPI*) GPIO15 to connect GND (*I²C*)
MO	MOSI *SPI* master output, slave input (output from master)
MI	MISO *SPI* master input, slave output (output from *TPM*)
IRQ	Active low, open drain, used by the to generate an interrupt.
CK	*SPI* serial clock (output from master)
CS0	*SPI* chip (or slave) select number 1, internal pull-up (active low; output from master)
CS1	*SPI* chip (or slave) select number 2, internal pull-up (active low; output from master)

1.8 STPM4RasPIV21 connection

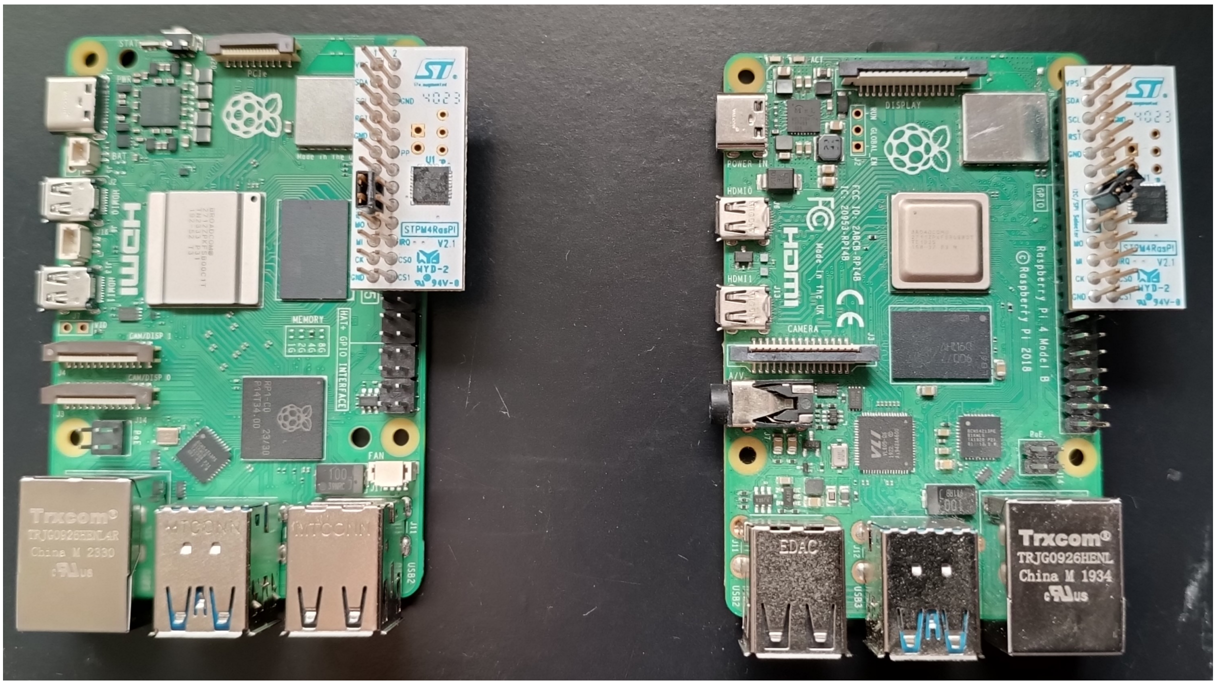
1.8.1 Raspberry Pi® 3, 4, and 5

The 40 GPIO header has the same definition and direction on the different versions (Raspberry Pi® 3, 4 or 5).

The STPM4RasPIV21 connection from pin 1 is broader than the Raspberry Pi® .

The Raspberry Pi® box cannot be embedded. The button access at the bottom is improved.

Figure 10. Raspberry Pi® 3, 4, and 5.

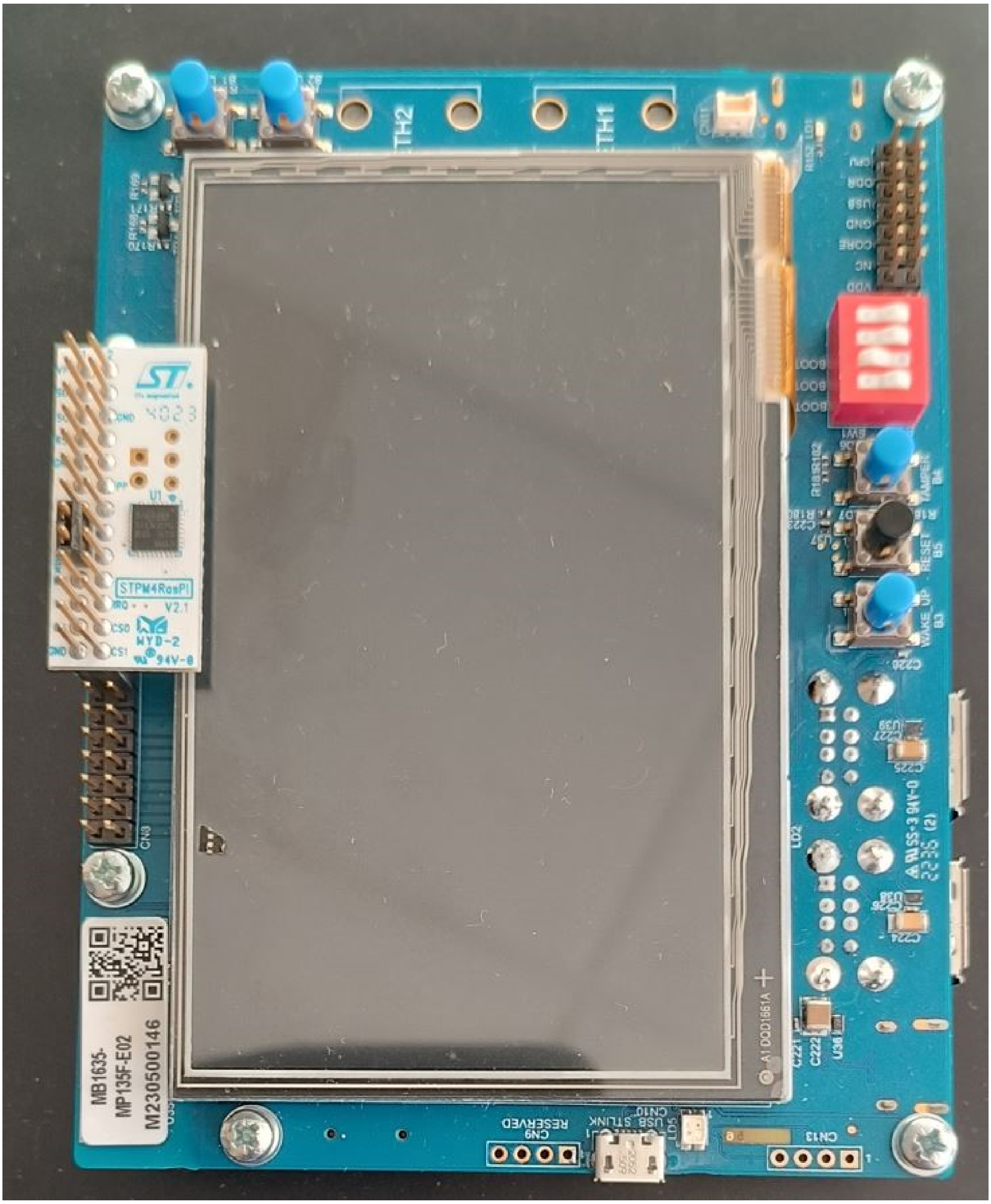


1.8.2 STM32MP135F-DK

The STM32MP135F-DK Discovery kit (STM32MP135F-DK) leverages the capabilities of the 1 GHz STM32MP135 microprocessors to allow users to develop easily applications using STM32 MPU OpenSTLinux Distribution software.

STPM4RASPIV21 is plugged on 40 GPIO header as shown in the figure below.

Figure 11. STM32MP135F-DK

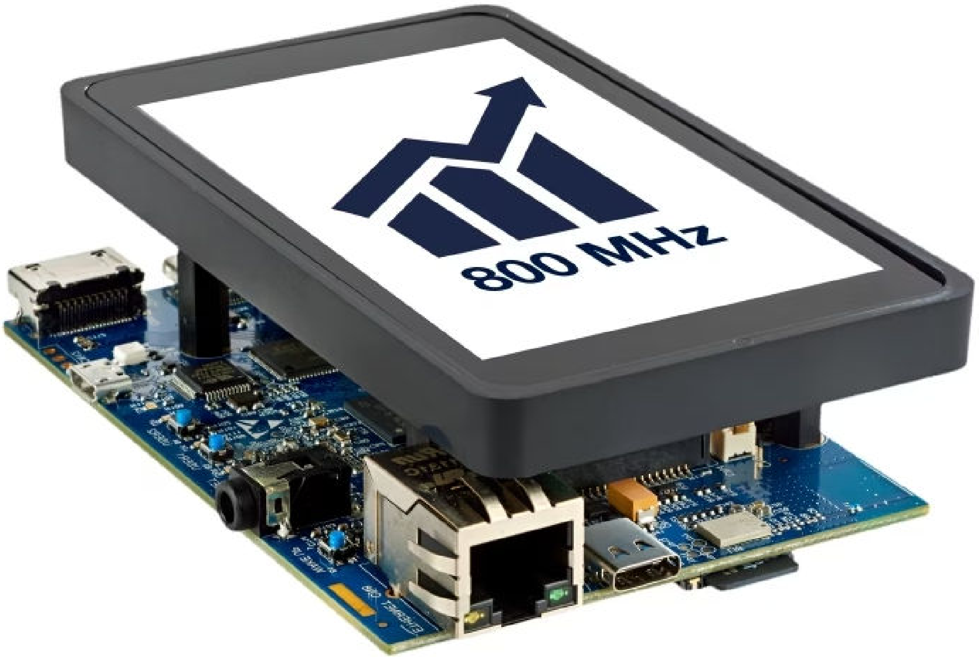


1.8.3 STM32MP157F-DK2

STM32MP157F-DK2 Discovery kits leverage the capabilities of the increased-frequency 800 MHz microprocessors in the STM32MP157 product line to allow users to develop applications easily using STM32 MPU OpenSTLinux Distribution software for the main processor, and STM32CubeMP1 software for the coprocessor.

The STM32MP157F 800MHz Discovery kit board include an ST-LINK embedded debug tool, LEDs, push-buttons, one Ethernet 1-Gbit/s connector, one USB Type-C® OTG connector, four USB Host Type-A connectors, one HDMI® transceiver, one stereo headset jack with analog microphone, and one microSD™ connector.

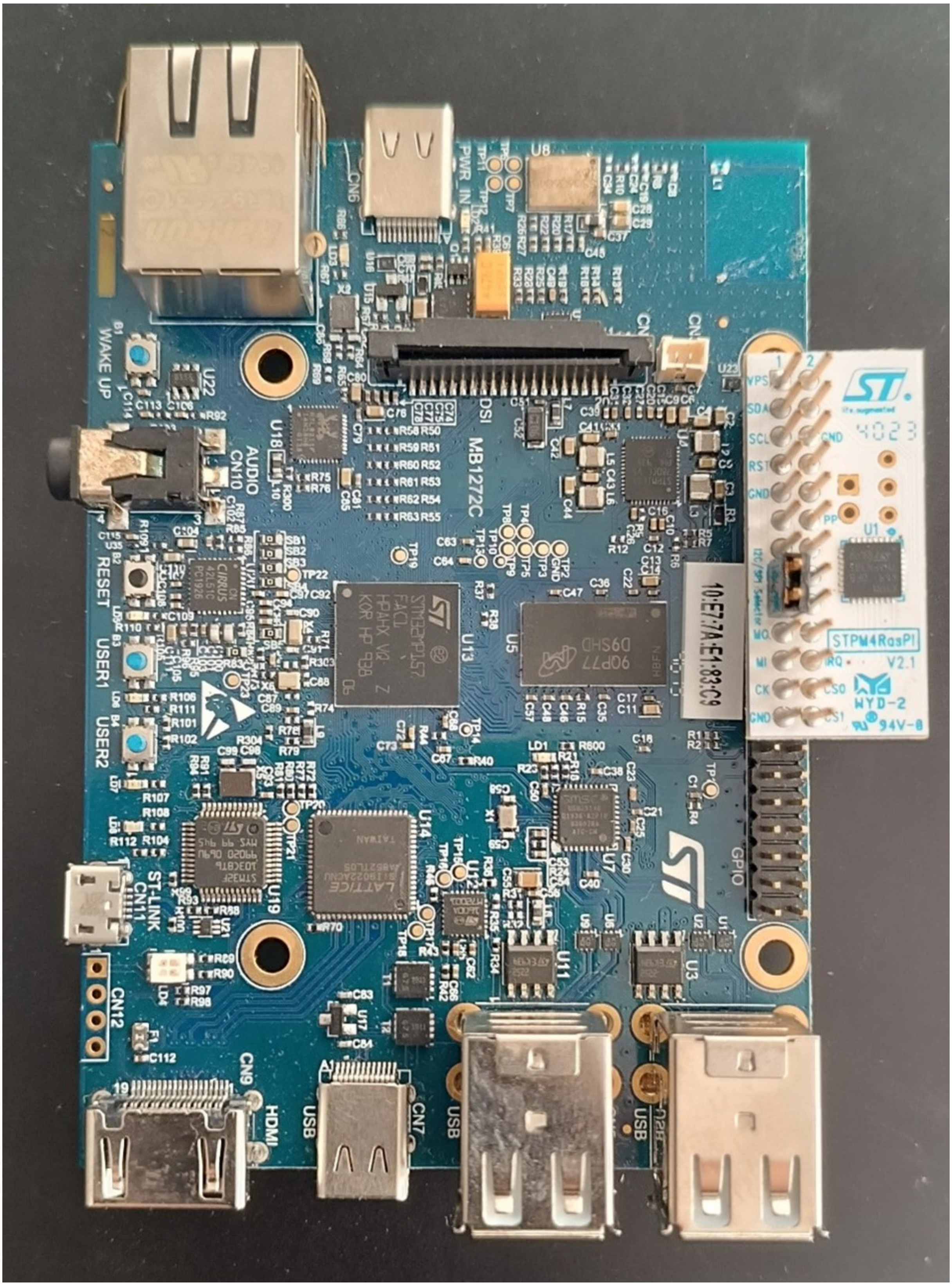
Figure 12. STM32MP157F-DK2



To expand the functionality of the and STM32MP157F-DK2 Discovery kits, two GPIO expansion connectors are also available for ARDUINO® and Raspberry Pi® shields.

STPM4RasPIV21 is connected to a Raspberry Pi® shield as shown in the figure below.

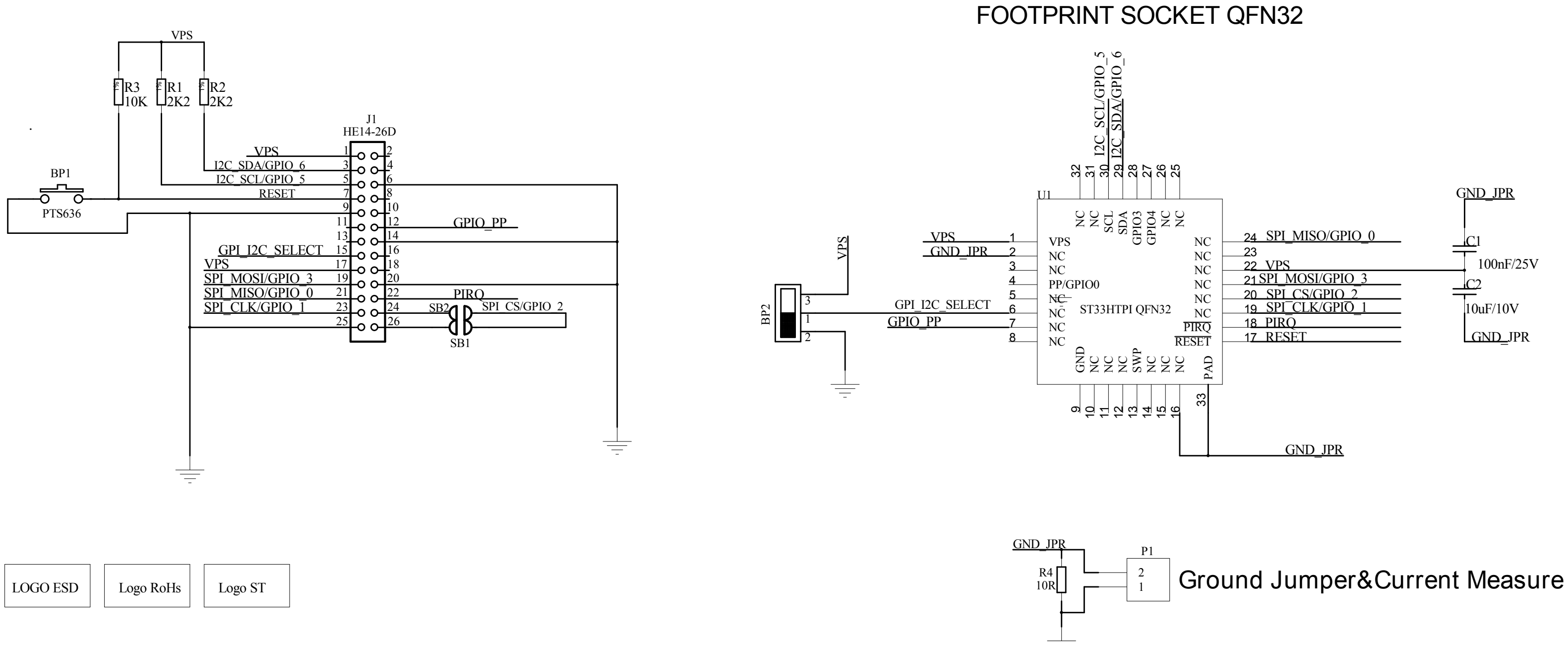
Figure 13. STM32MP157F-DK2 plug-in



2 STPM4RasPIV21 schematics

The STPM4RasPIV21 board schematics are illustrated in the figure below.

Figure 14. STPM4RasPIV21 board schematics



3 Linux®TPM activation

The table below describes *TPM* activation according to the Linux® kernel.

Table 3. **Linux®*TPM* activation**

Linux® kernel	TPM
6.1 and above	[TCG-TPM-I2C-DRV main]
5.10 to 6.0	[TCG-TPM-I2C-DRV 5.10]
5.4 to 5.9	[TCG-TPM-I2C-DRV 5.4]

TPM activation over STM32MP1xx devices is facilitated. X-LINUX-TPM is a Yocto layer to support *TPM* driver and applications in *I²C* and *SPI*.

For further information on *TPM* integration, refer to the X-LINUX-TPM wiki and to *Integrating the STSAFE-TPM trusted platform modules with Linux®* (AN5714) application note in Section 4: Linux®TPM application.

Note: *The devices are referred to as STM32MP1xx implies that either the STM32MP135F or the STM32MP157F can be used.*

4 Linux®TPM application

For further information on the Linux® *TPM* application, refer to the following documentation.

Table 4. **Reference documentation**

Resource type	Resource location
Application note	AN5714 application note
Databrief	STPM4RasPI
GitHub	[TCG-TPM-I2C-DRV main]
GitHub	[TCG-TPM-I2C-DRV 5.4]
GitHub	[TCG-TPM-I2C-DRV 5.10]
PTP standard specification	[PTP standard specification]
Product page	ST33KTPM2X
Product page	ST33KTPM2XSPI
Product page	ST33KTPM2I
Wiki article	X-LINUX-TPM
GitHub	X-LINUX-TPM

Note: Some of the above-mentioned URLs belong to a third-party. Active at document publication, STMicroelectronics shall not be liable for any change, move, or inactivation of the URL or the referenced material.

5 Ordering information

The STPM4RasPIV21 extension board can be ordered using the commercial product names listed in the table below.

Table 5. **Ordering information**

Commercial product	Description	TPM part numbers
SC-KTPM-RASPIKG9	*TCG* TPM2.0 spec 1.59, firmware version 9.257, SPI, and *I²C* interface.	ST33KTPM2X32DKG9
SC-KTPM-RASPIZA9	*TCG* TPM2.0 spec 1.59, firmware version 10.257, SPI, and *I²C* interface for industrial applications	ST33KTPM2I3WBZA9

Note: For the description of the soldered products and details on how to order them, refer to the data briefs of the corresponding TPM devices (TPM part numbers defined in the above table).

Revision history

Table 6. **Document revision history**

Date	Revision	Changes
30-Jan-2024	1	Initial release.
30-Jul-2024	2	Added: • Section 2: STPM4RasPIV21 schematics • Glossary Updated: • Document title • Section Features • Section 1: STPM4RasPIV21 main features • Section 1.2: Raspberry *SPI* / *I²C* connectivity by *GPIO* • Section 1.5: Bus interface selection • Section 1.6: Configuration of the SPI chip selection • Section 1.7: Signal marking on PCB • Section 1.8.3: STM32MP157F-DK2 • Section 3: Linux®TPM activation • Section 4: Linux®TPM application • Section 5: Ordering information

Glossary

GPIO General purpose input/output

I^{2}C Inter-integrated circuit

PCB Printed-circuit board

PP Physical presence

PTP Platform *TPM* Profile

SPI Serial peripheral interface

TCG Trusted Computing Group®

TPM Trusted platform module

Contents

1 **STPM4RasPIV21 main features** **2**

1.1 STPM4RasPIV21 introduction 2

1.2 Raspberry *SPI* / *I²C* connectivity by *GPIO* 3

1.3 TPM power consumption 4

1.4 TPM reset button 4

1.5 Bus interface selection 4

1.5.1 Bus interface selection using a jumper 4

1.5.2 Bus interface selection using a switch slide 7

1.6 Configuration of the SPI chip selection 7

1.7 Signal marking on PCB 8

1.8 STPM4RasPIV21 connection 9

1.8.1 Raspberry Pi® 3, 4, and 5 9

1.8.2 STM32MP135F-DK 10

1.8.3 STM32MP157F-DK2 11

2 **STPM4RasPIV21 schematics** **13**

3 **Linux®TPM activation** **14**

4 **Linux®TPM application** **15**

5 **Ordering information** **16**

Revision history **17**

Glossary **18**

List of figures

Figure 1. STPM4RasPIV21 . . . 2
Figure 2. Raspberry Pi *GPIO* . . . 3
Figure 3. P1 header location . . . 4
Figure 4. Reset button . . . 4
Figure 5. Use of the I2C/SPI jumper for the *SPI* interface selection . . . 5
Figure 6. Use of the I2C/SPI jumper for the *I²C* interface selection . . . 6
Figure 7. Use of the switch slide for interface selection . . . 7
Figure 8. SPI chip selection configuration . . . 7
Figure 9. Signal marking on *PCB* . . . 8
Figure 10. Raspberry Pi® 3, 4, and 5. . . . 9
Figure 11. STM32MP135F-DK . . . 10
Figure 12. STM32MP157F-DK2 . . . 11
Figure 13. STM32MP157F-DK2 plug-in. . . . 12
Figure 14. STPM4RasPIV21 board schematics . . . 13

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.