Guidelines for entering RMA state on STM32MP1 Series MPUs

Introduction

STM32MP1 Series microprocessors include STM32MP15xx and STM32MP13xx devices..

This application note provides information to support the return material analysis state entering process, referred to as RMA in this document.

1 General information

This document applies to STM32MP1 Series microprocessors based on Arm® Cortex® cores

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Reference documents

Table 1. Reference documents

Reference	Document title
STM32MP13xx	
AN5474	Getting started with STM32MP13x lines hardware development
DS13878	Arm® Cortex®-A7 up to 1 GHz, 1×ETH, 1×ADC, 24 timers, audio
DS13877	Arm® Cortex®-A7 up to 1 GHz, 1×ETH, 1×ADC, 24 timers, audio, crypto and adv. security
DS13876	Arm® Cortex®-A7 up to 1 GHz, 2×ETH, 2×CAN FD, 2×ADC, 24 timers, audio
DS13875	Arm® Cortex®-A7 up to 1 GHz, 2×ETH, 2×CAN FD, 2×ADC, 24 timers, audio, crypto and adv. security
DS13874	Arm® Cortex®-A7 up to 1 GHz, LCD-TFT, camera interface, 2×ETH, 2×CAN FD, 2×ADC, 24 timers, audio
DS13483	Arm® Cortex®-A7 up to 1 GHz, LCD-TFT, camera interface, 2×ETH, 2×CAN FD, 2×ADC, 24 timers, audio, crypto and adv. security
RM0475	STM32MP13xx advanced Arm®-based 32-bit MPUs
STM32MP15xx	
AN5031	Getting started with STM32MP151, STM32MP153 and STM32MP157 line hardware development
DS12500	Arm® Cortex®-A7 800 MHz + Cortex®-M4 MPU, TFT, 35 comm. interfaces, 25 timers, adv. analog
DS12501	Arm® Cortex®-A7 800 MHz + Cortex®-M4 MPU, TFT, 35 comm. interfaces, 25 timers, adv. analog, crypto
DS12502	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU, TFT, 37 comm. interfaces, 29 timers, adv. analog
DS12503	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU, TFT, 37 comm. interfaces, 29 timers, adv. analog, crypto
DS12504	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU, 3D GPU, TFT/DSI, 37 comm. interfaces, 29 timers, adv. analog
DS12505	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU, 3D GPU, TFT/DSI, 37 comm. interfaces, 29 timers, adv. analog, crypto
RM0441	STM32MP151 advanced Arm®-based 32-bit MPUs
RM0442	STM32MP153 advanced Arm®-based 32-bit MPUs
RM0436	STM32MP157 advanced Arm®-based 32-bit MPUs

Terms and acronyms

Table 2. Acronyms definition

Term	Definition
FAR	Failure analysis request: flow used to return suspicious device for analysis to STMicroelectronics. To enhance the full testability of the device during such analysis, the device must be in RMA state.
JTAG	Joint test action group (debug interface)
PMIC	External power-management circuit that provides various platform power supplies, with large controllability through signals and serial interface.
RMA[(1)]	Return material analysis: specific device state in the life cycle that allows activation of full-test mode as needed by STMicroelectronics for failure analysis purpose.

1. *In this document, the RMA acronym does not refer anywhere to “return material acceptance” that is the flow used to return non-used parts (customer stock for example).*

2 RMA state within the FAR flow

The FAR flow consists in returning a device to STMicroelectronics for deeper failure analysis in case of a suspected quality issue. The part must be returned testable to ST so that the analysis can be performed.

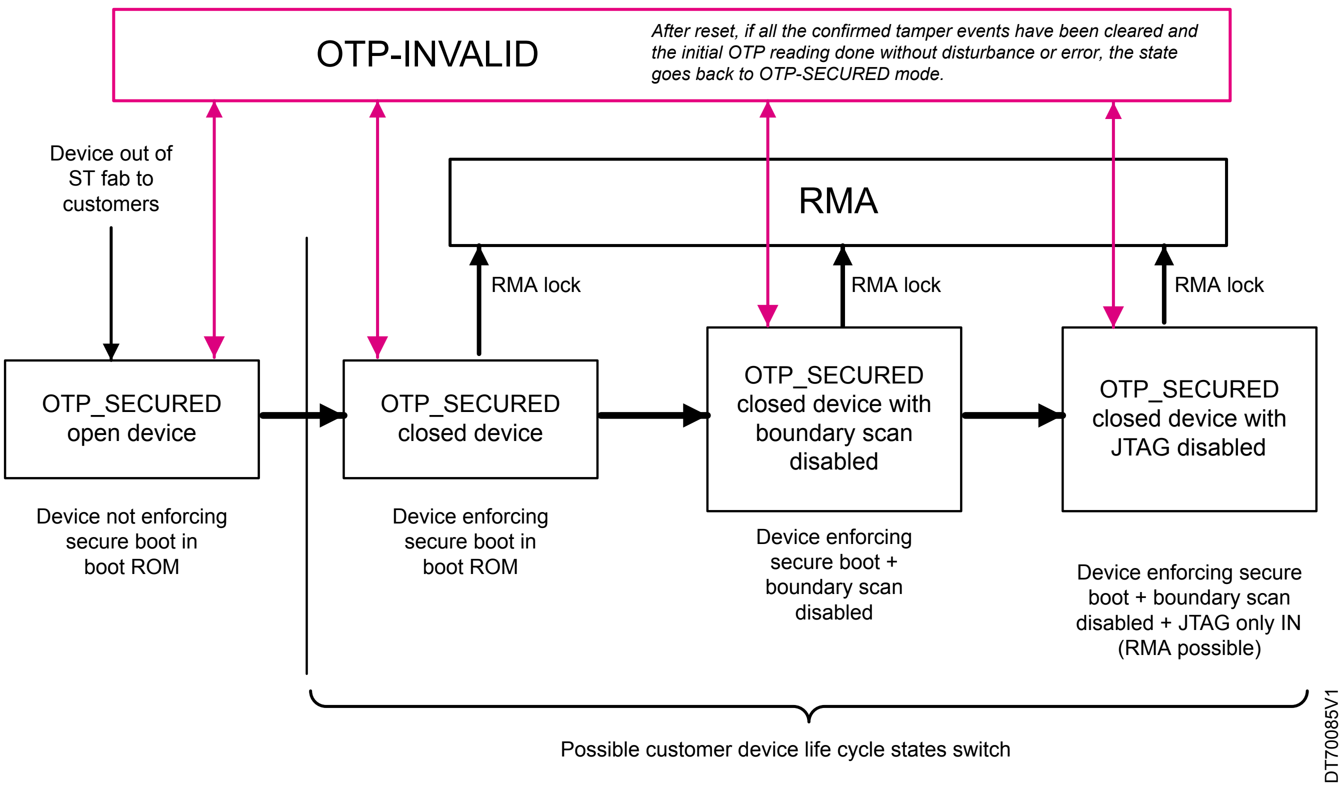
- The part must be in RMA state
- The part must be physically compatible with the original device (ball size, pitch, etc.)

2.1 STM32MP13xx product life cycle

On STM32MP13xx devices, before returning the device, the customer must enter into RMA state with a customer predefined 32-bit password entered through the JTAG (see Section 3). Once entered in RMA state, the device is not anymore usable for production (see Figure 1) and the full-test mode is activated for STMicroelectronics to carry on investigation while all the customer secrets (upper OTP as described in reference manual) are kept inaccessible by the hardware.

The figure below shows the product life cycle of STM32MP13xx devices. It shows that once the RMA state is entered the device cannot go back to other modes.

Figure 1. Product life cycle for STM32MP13xx devices

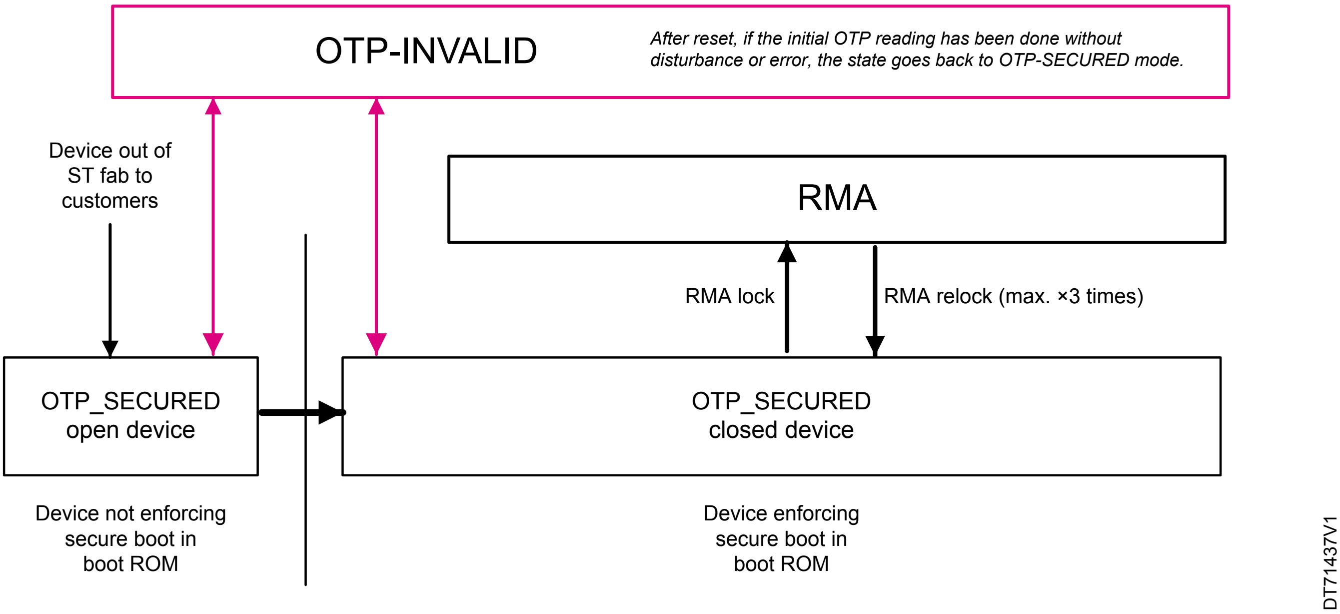


2.2 STM32MP15xx product life cycle

On STM32MP15xx devices, before returning the device, the customer must enter into RMA state with a customer predefined 15-bit password entered through the JTAG (see Section 3). Once entered in RMA state, the device can go back to SECURE_CLOSED state by entering a customer predefined "RMA_RELOCK" password. Only 3 RMA to RMA_RELOCKED transition state trials are allowed (see Figure 2). In RMA state, the full-test mode is activated for STMicroelectronics to carry on investigation while all the customer secrets (upper OTP as described in reference manual) are kept inaccessible by the hardware.

The figure below shows the product life cycle of STM32MP15x devices.

Figure 2. Product life cycle for STM32MP15xx devices



3 RMA state board constraints

To activate the RMA state, the following constraints are required.

The JTAG access should be available

The signals NJTRST and JTDI, JTCK, JTMS, JTDO (pin PH4, PH5, PF14, PF15 on STM32MP13xx devices) must be accessible. On some tools, the JTDO is not necessary (for example, Trace32) on other like OpenOCD the tool checks the device JTAG ID via JTDO before executing the JTAG sequence.

The V_{DDCORE} and V_{DD} power supplies should not be powered off when the NRST pin is activated

On ST reference design, the NRST activates a power cycle of the STPMIC1x or external discrete components power regulators. A possible implementation is shown in the reference design example provided in the application note *Getting started with STM32MP13x lines hardware development* (AN5474) . Figure 3 and Figure 4 are simplified versions that only show the RMA state related components. The same applies for STM32MP15xx devices.

Figure 3. RMA state additional components on STPMIC based design

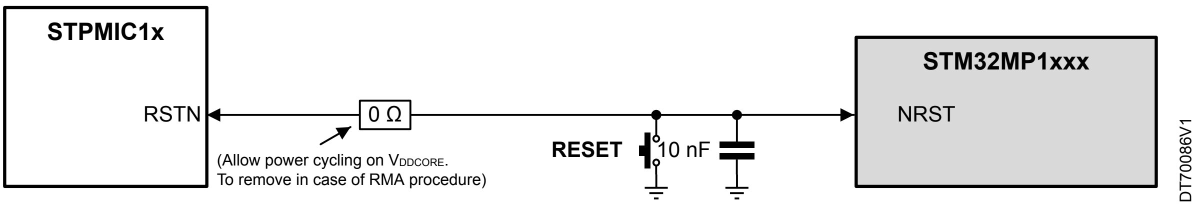
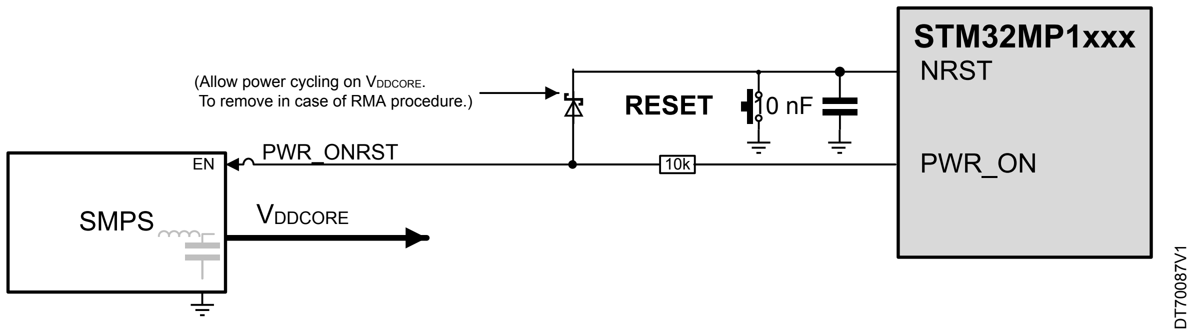


Figure 4. RMA state additional components on discrete components supply based design



A simple board with only the JTAG pin and appropriate socket can be used for RMA password purposes only (in case it is not possible to access JTAG on the production board). In such case the customer must first unsolder the device from the production board and repopulate the package balls.

The board must have the STM32MP1xxx pins listed in Table 3 connected as indicated . Other pins can be left floating.

Table 3. Pin connection for simple board used for RMA password entering

Pin name (signal)		Connected to	Comment
STM32MP13xx	STM32MP15xx		
JTAG and reset			
NJTRST	NJRST	JTAG connector	-
PH4 (JTDI)	JTDI		-
PH5 (JTDO)	JTDO		Not needed on some debug tool like Trace32
PF14 (JTCK)	JTCK		-
PF15 (JTMS)	JTMS		-
NRST	NRST	Reset button	With 10 nF capacitor to V_{SS}
Power supplies			
VDDCORE, VDDCPU	VDDCORE	External supply	Refer to product datasheet for typical value
VDD, VDDSD1, VDDSD2, VDD_PLL, VDD_PLL2, VBAT, VDD_ANA, PDR_ON	VDD, VDD_PLL, VDD_PLL2, VBAT, VDD_ANA, PDR_ON, PDR_ON_CORE	3.3 V external supply	Should be available first and removed last (can be together with other supplies)
VDDA, VREF+, VDD3V3_USBHS, VDDQ_DDR	VDDA, VREF+, VDD3V3_USBHS, VDDQ_DDR, VDD_DSI, VDD1V2_DSI_REG, VDD3V3_USBFS	0	ADC, VREFBUF, USB, DDR not used
VSS, VSS_PLL, VSS_PLL2, VSSA, VSS_ANA, VREF-, VSS_USBHS	VSS, VSS_PLL, VSS_PLL2, VSSA, VSS_ANA, VREF-, VSS_USBHS, VSS_DSI	0	-
VDDA1V8_REG, VDDA1V1_REG	VDDA1V8_REG, VDDA1V1_REG	floating	-
Other			
BYPASS_REG1V8	BYPASS_REG1V8	0	1V8 regulator enabled by default (REG18E = 1)
PC15- OSC32_OUT	PC15- OSC32_OUT	floating	External oscillators not used (boot ROM to use HSI internal oscillator)
PC14- OSC32_IN	PC14- OSC32_IN		
PH0-OSC_IN	PH0-OSC_IN		
PH1-OSC_OUT	PH1-OSC_OUT		
USB_RREF	USB_RREF	floating	USB not used
PI6 (BOOT2)	BOOT2	X	Entering in the RMA state works whatever the boot[2:0] values
PI5 (BOOT1)	BOOT1	X	
PI4 (BOOT0)	BOOT0	X	
-	NRST_CORE	10 nF to VSS	Internal pull-up on NRST_CORE
PA13 (BOOTFAILN)	PA13 (BOOTFAILN)	LED	Optional

4 Prior requirements to allows future RMA state entering

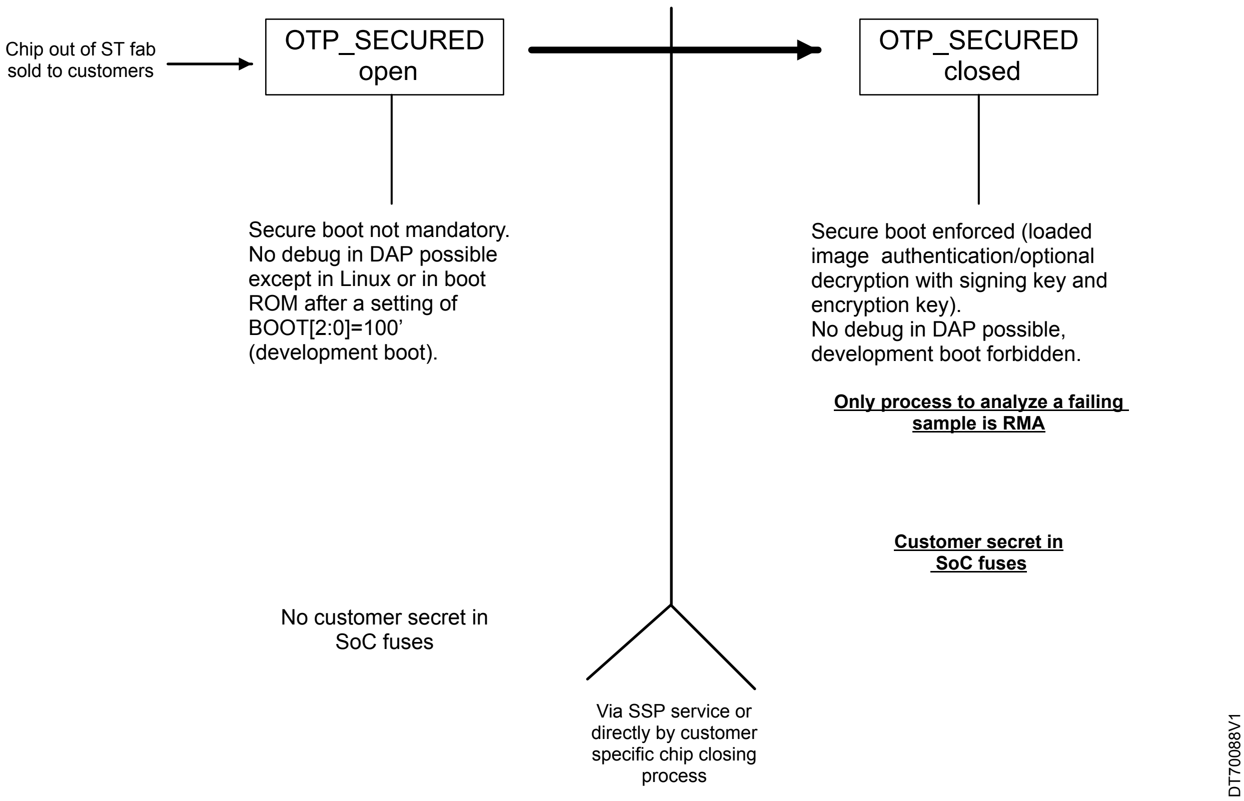
The possibility to enter RMA state must be set up by the customer by entering a password during customer production after secret provisioning

- The device when shipped from STMicroelectronics is in OTP_SECURED open state.
- The device contains ST secrets that are protected by boot ROM, and no customer secret.
- At reset or after boot ROM execution, DAP access can be reopened by Linux or by boot ROM “development boot” mode (OTP_SECURED open + boot pins BOOT[2:0]=1b100 + reset).
- While in OTP_SECURED open, the customer must provision its secrets in OTP:
  - directly by customer at own risk or
  - securely via the encrypted channel using the “SSP feature” of boot ROM together with STM32 tools.
- At the end of secrets provisioning, the customer can fuse:
  - On STM32MP13xx a 32 bit RMA password in OTP_CFG56 (password should be ≠ 0).
  - On STM32MP15xx a 15 bit RMA password in OTP_CFG56[14:0], a RMA_RELOCK password in OTP_CFG56[29:15].

  The password should be different than 0.
- Set the OTP_CFG56 as “permanent programming lock” to avoid later programming at 0xFFFFFF and allow entering the RMA state without knowledge of the initial password.
- Verify the correct programming of the OTP_CFG56 by checking the BSEC_OTP_STATUS register.
- Finally, the device is switched to OTP_SECURED closed:
  - On STM32MP13xx by fusing OTP_CFG0[3] = 1 and OTP_CFG0[5] = 1.
  - On STM32MP15xx by fusing OTP_CFG0[6] = 1.

  The device can be reopened in RMA state for investigation by STMicroelectronics
- When the device is in OTP_SECURED closed state, “development boot” is no more possible.

Figure 5. Switching to OTP_SECURED closed



5 RMA state entering details

As mentioned previously, the RMA state is used to reopen securely the full test mode without any exposure of customer provisioned secrets. This is done thanks to the functional JTAG inputs while all the customer secrets are kept inaccessible by the hardware.

In case there is a requirement for analysis on a failing sample there is the need to go to RMA state (see Figure 5. Switching to OTP_SECURED closed), which secures customer secrets and reopens debug secure and non-secure in DAP.

1. The customer shifts in BSEC_JTAGIN register the RMA password using JTAG (only values different from 0 are accepted).
2. The customer resets the device (NRST pin).

Note: During this step, the password in BSEC_JTAGIN register must not be erased. Thus, the NRST must not shut down the V_{DD} nor the V_{DDCORE} power supplies. It should also not be connected to the NJTRST pin. In case STPMIC1x is used, it might be mandatory to mask the power supplies during the reset. This is done by programming the STPMIC1x mask option register (BUCKS_MRST_CR) or removing the resistor added for RMA on the board between STPMICx RSTn and STM32MP1xxx NRST (see Figure 3).

3. The boot ROM is invoked and checks the RMA password entered in BSEC_JTAGIN with OTP_CFG56.RMA_PASSWORD:
   - If the passwords match, the sample becomes an RMA_LOCK sample (forever on STM32MP13xx).
   - If the passwords do not match, the sample stays in the OTP_SECURED closed state and an RMA "reopening trials" counter is incremented in OTP.

   Note: Only three RMA reopening trials are authorized. After three failed trials, RMA reopening is no more possible. The device stays in its actual life cycle state.
4. The customer resets a second time the sample via NRST pin:
   - the LED on PA13 is on (if connected)
   - the DAP debug access is reopened.
5. The device can be sent to STMicroelectronics.
6. After reset (NRST pin or any system reset), the boot ROM is invoked:
   - It detects that OTP8.RMA_LOCK = 1 (RMA locked sample).
   - It secures all STMicroelectronics and customer secrets.
   - It reopens DAP debug access in secure and non-secure.

While in RMA state the part is ignoring the Boot pins and is not able to boot from external flash nor USB/UART.

6 RMA unlock details

On STM32MP15xx it is possible to unlock the device from RMA and go back to SECURE_CLOSED state.

In BSEC_JTAGIN register, the customer shifts the RMA unlock password using JTAG (only values different from 0 are accepted)

- The customer resets the device (NRST pin).

Note: Only three RMA Unlock trials are authorized. After three failed trials, RMA unlock is no more possible. The device stays in its RMA life cycle state.

- The customer resets a second time the sample via NRST pin:
  – the LED on PA13 is on (if connected),
  – the device is in SECURE_CLOSED state (DAP debug access is closed).

7 RMA state entering JTAG script examples

STM32MP13xx script examples to enter the password and enter the RMA state are available in a separated zip file. They can be used with Trace32, OpenOCD using STLINK probe, OpenOCD using CMSIS-DAP compatible probe (for example ULink2). Information can be found at www.st.com. Refer to STM32MP13xx product “CAD resources” in the “board manufacturing specification” section.

Similar examples can be derived for STM32MP15xx devices. An example to enter RMA state and to exit RMA state for Trace32 is available in a separated zip file. Information can be found at www.st.com. Refer to STM32MP15x product “CAD resources” in the “board manufacturing specification” section.

Revision history

Table 4. **Document revision history**

Date	Version	Changes
13-Feb-2023	1	Initial release.

Contents

List of tables

List of figures