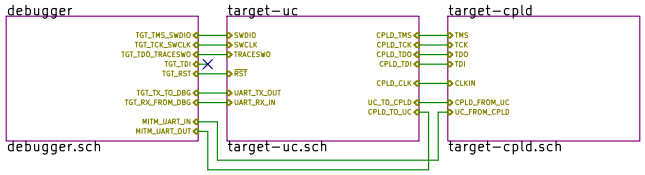


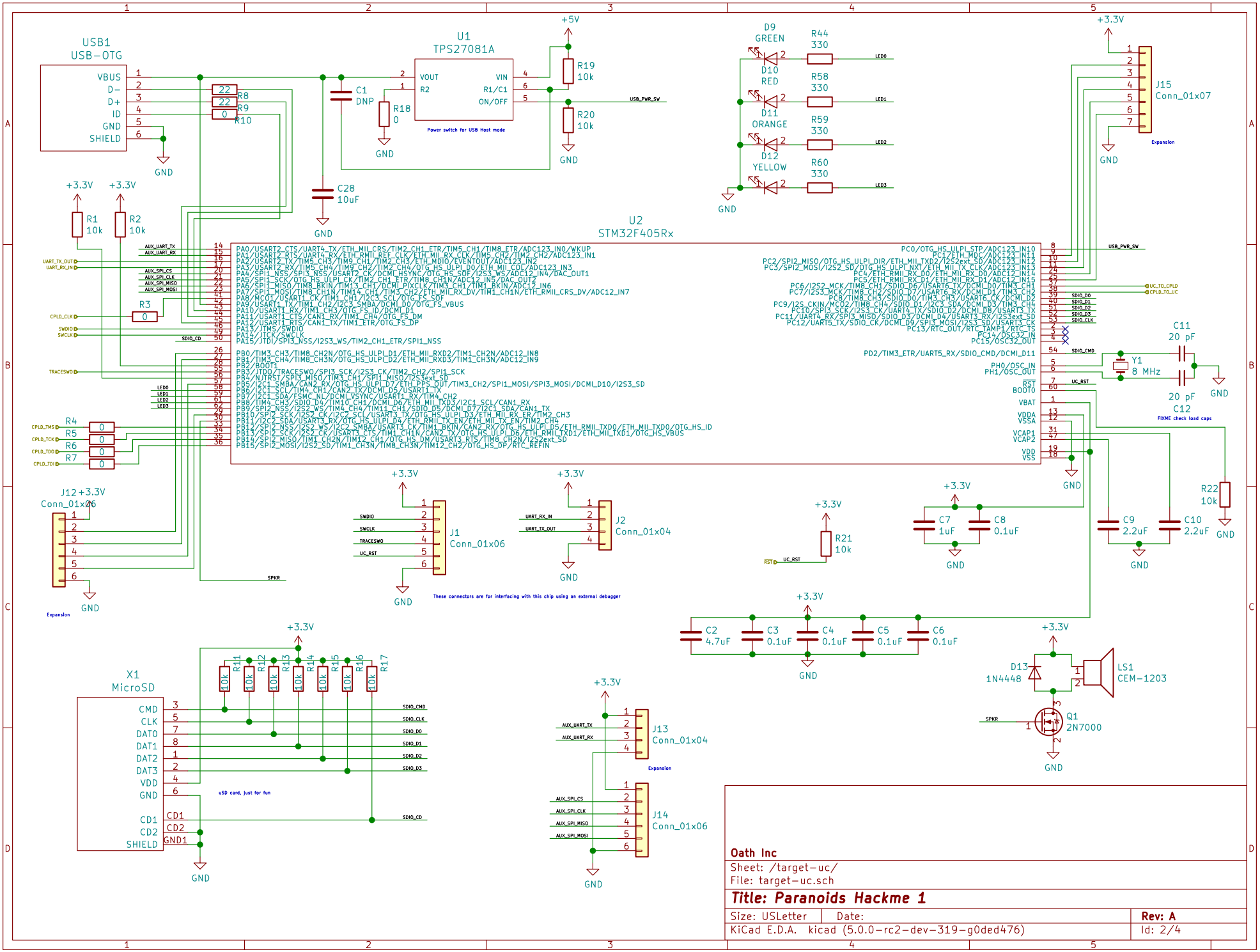
Oath Inc

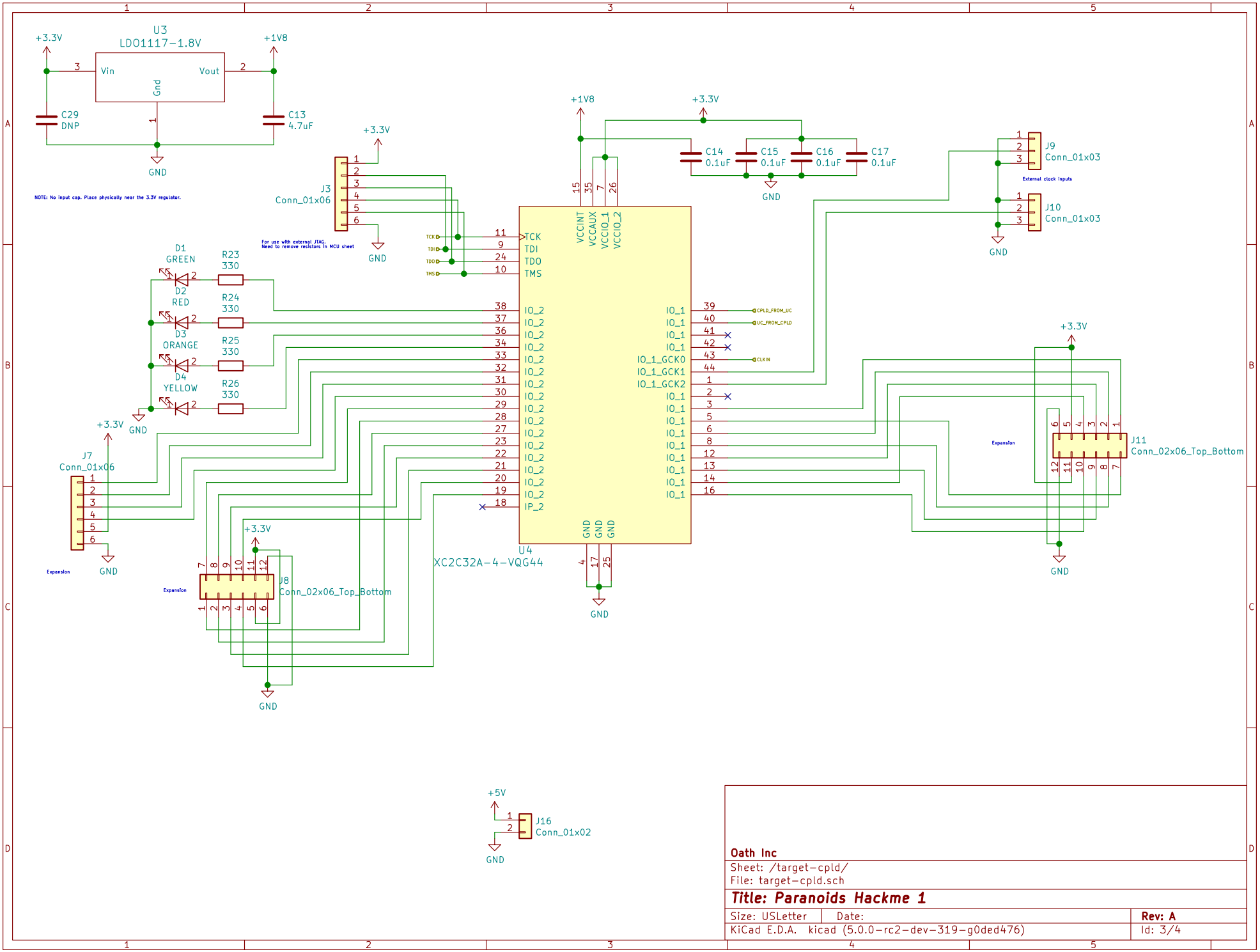
Sheet: /

File: paranoids-hackme-1.sch

Title: Paranoids Hackme 1

Size: USLetter	Date:	**Rev: A**
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)		Id: 1/4


USB1
USB-OTG
VBUS
D-
D+
ID
GND
SHIELD
R8 22
R9 22
R10 0
C1 DNP
R18 0
U1
TPS27081A
VOUT
R2
VIN
R1/C1
ON/OFF
Power switch for USB Host mode
R19 10k
R20 10k
USB_PWR_SW
C28 10uF
D9 GREEN
D10 RED
D11 ORANGE
D12 YELLOW
R44 330
R58 330
R59 330
R60 330
LED0
LED1
LED2
LED3
J15
Conn_01x07
Expansion
R1 10k
R2 10k
R3 0
R4 0
R5 0
R6 0
R7 0
U2
STM32F405Rx
PA0/USART2_CTS/UART4_TX/ETH_MII_CRS/TIM2_CH1_ETR/TIM5_CH1/TIM8_ETR/ADC123_IN0/WKUP
PA1/USART2_RTS/UART4_RX/ETH_RMII_REF_CLK/ETH_MII_RX_CLK/TIM5_CH2/TIM2_CH2/ADC123_IN1
PA2/USART2_TX/TIM5_CH3/TIM9_CH1/TIM2_CH3/ETH_MDIO/EVENTOUT/ADC123_IN2
PA3/USART2_RX/TIM5_CH4/TIM9_CH2/TIM2_CH4/OTG_HS_ULPI_D0/ETH_MII_COL/ADC123_IN3
PA4/SPI1_NSS/SPI3_NSS/USART2_CK/DCMI_HSYNC/OTG_HS_SOF/I2S3_WS/ADC12_IN4/DAC_OUT1
PA5/SPI1_SCK/OTG_HS_ULPI_CK/TIM2_CH1_ETR/TIM8_CH1N/ADC12_IN5/DAC_OUT2
PA6/SPI1_MISO/TIM8_BKIN/TIM13_CH1/DCMI_PIXCLK/TIM3_CH1/TIM1_BKIN/ADC12_IN6
PA7/SPI1_MOSI/TIM8_CH1N/TIM14_CH1/TIM3_CH2/ETH_MII_RX_DV/TIM1_CH1N/ETH_RMII_CRS_DV/ADC12_IN7
PA8/MCO1/USART1_CK/TIM1_CH1/I2C3_SCL/OTG_FS_SOF
PA9/USART1_TX/TIM1_CH2/I2C3_SMBA/DCMI_D0/OTG_FS_VBUS
PA10/USART1_RX/TIM1_CH3/OTG_FS_ID/DCMI_D1
PA11/USART1_CTS/CAN1_RX/TIM1_CH4/OTG_FS_DM
PA12/USART1_RTS/CAN1_TX/TIM1_ETR/OTG_FS_DP
PA13/JTMS/SWDIO
PA14/JTCK/SWCLK
PA15/JTDI/SPI3_NSS/I2S3_WS/TIM2_CH1_ETR/SPI1_NSS
PB0/TIM3_CH3/TIM8_CH2N/OTG_HS_ULPI_D1/ETH_MII_RXD2/TIM1_CH2N/ADC12_IN8
PB1/TIM3_CH4/TIM8_CH3N/OTG_HS_ULPI_D2/ETH_MII_RXD3/TIM1_CH3N/ADC12_IN9
PB2/BOOT1
PB3/JTDO/TRACESWO/SPI3_SCK/I2S3_CK/TIM2_CH2/SPI1_SCK
PB4/NJTRST/SPI3_MISO/TIM3_CH1/SPI1_MISO/I2S3ext_SD
PB5/I2C1_SMBA/CAN2_RX/OTG_HS_ULPI_D7/ETH_PPS_OUT/TIM3_CH2/SPI1_MOSI/SPI3_MOSI/DCMI_D10/I2S3_SD
PB6/I2C1_SCL/TIM4_CH1/CAN2_TX/DCMI_D5/USART1_TX
PB7/I2C1_SDA/FSMC_NL/DCMI_VSYNC/USART1_RX/TIM4_CH2
PB8/TIM4_CH3/SDIO_D4/TIM10_CH1/DCMI_D6/ETH_MII_TXD3/I2C1_SCL/CAN1_RX
PB9/SPI2_NSS/I2S2_WS/TIM4_CH4/TIM11_CH1/SDIO_D5/DCMI_D7/I2C1_SDA/CAN1_TX
PB10/SPI2_SCK/I2S2_CK/I2C2_SCL/USART3_TX/OTG_HS_ULPI_D3/ETH_MII_RX_ER/TIM2_CH3
PB11/I2C2_SDA/USART3_RX/OTG_HS_ULPI_D4/ETH_RMII_TX_EN/ETH_MII_TX_EN/TIM2_CH4
PB12/SPI2_NSS/I2S2_WS/I2C2_SMBA/USART3_CK/TIM1_BKIN/CAN2_RX/OTG_HS_ULPI_D5/ETH_RMII_TXD0/ETH_MII_TXD0/OTG_HS_ID
PB13/SPI2_SCK/I2S2_CK/USART3_CTS/TIM1_CH1N/CAN2_TX/OTG_HS_ULPI_D6/ETH_RMII_TXD1/ETH_MII_TXD1/OTG_HS_VBUS
PB14/SPI2_MISO/TIM1_CH2N/TIM12_CH1/OTG_HS_DM/USART3_RTS/TIM8_CH2N/I2S2ext_SD
PB15/SPI2_MOSI/I2S2_SD/TIM1_CH3N/TIM8_CH3N/TIM12_CH2/OTG_HS_DP/RTC_REFIN
PC0/OTG_HS_ULPI_STP/ADC123_IN10
PC1/ETH_MDC/ADC123_IN11
PC2/SPI2_MISO/OTG_HS_ULPI_DIR/ETH_MII_TXD2/I2S2ext_SD/ADC123_IN12
PC3/SPI2_MOSI/I2S2_SD/OTG_HS_ULPI_NXT/ETH_MII_TX_CLK/ADC123_IN13
PC4/ETH_RMII_RX_D0/ETH_MII_RX_D0/ADC12_IN14
PC5/ETH_RMII_RX_D1/ETH_MII_RX_D1/ADC12_IN15
PC6/I2S2_MCK/TIM8_CH1/SDIO_D6/USART6_TX/DCMI_D0/TIM3_CH1
PC7/I2S3_MCK/TIM8_CH2/SDIO_D7/USART6_RX/DCMI_D1/TIM3_CH2
PC8/TIM8_CH3/SDIO_D0/TIM3_CH3/USART6_CK/DCMI_D2
PC9/I2S_CKIN/MCO2/TIM8_CH4/SDIO_D1/I2C3_SDA/DCMI_D3/TIM3_CH4
PC10/SPI3_SCK/I2S3_CK/UART4_TX/SDIO_D2/DCMI_D8/USART3_TX
PC11/UART4_RX/SPI3_MISO/SDIO_D3/DCMI_D4/USART3_RX/I2S3ext_SD
PC12/UART5_TX/SDIO_CK/DCMI_D9/SPI3_MOSI/I2S3_SD/USART3_CK
PC13/RTC_OUT1/RTC_TAMP1/RTC_TS
PC14/OSC32_IN
PC15/OSC32_OUT
PD2/TIM3_ETR/UART5_RX/SDIO_CMD/DCMI_D11
PH0/OSC_IN
PH1/OSC_OUT
NRST
BOOT0
VBAT
VDDA
VSSA
VCAP1
VCAP2
VDD
VSS
Y1 8 MHz
C11 20 pF
C12 20 pF
FIXME check load caps
R22 10k
C7 1uF
C8 0.1uF
C9 2.2uF
C10 2.2uF
R21 10k
C2 4.7uF
C3 0.1uF
C4 0.1uF
C5 0.1uF
C6 0.1uF
J12
Conn_01x06
Expansion
J1
Conn_01x06
J2
Conn_01x04
These connectors are for interfacing with this chip using an external debugger
X1
MicroSD
CMD
CLK
DAT0
DAT1
DAT2
DAT3
VDD
GND
CD1
CD2
GND1
SHIELD
R11 10k
R12 10k
R13 10k
R14 10k
R15 10k
R16 10k
R17 10k
uSD card, just for fun
D13 1N4448
LS1 CEM-1203
Q1 2N7000
J13
Conn_01x04
J14
Conn_01x06
Oath Inc
Sheet: /target-uc/
File: target-uc.sch
Title: Paranoids Hackme 1
Size: USLetter
Date:
Rev: A
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)
Id: 2/4



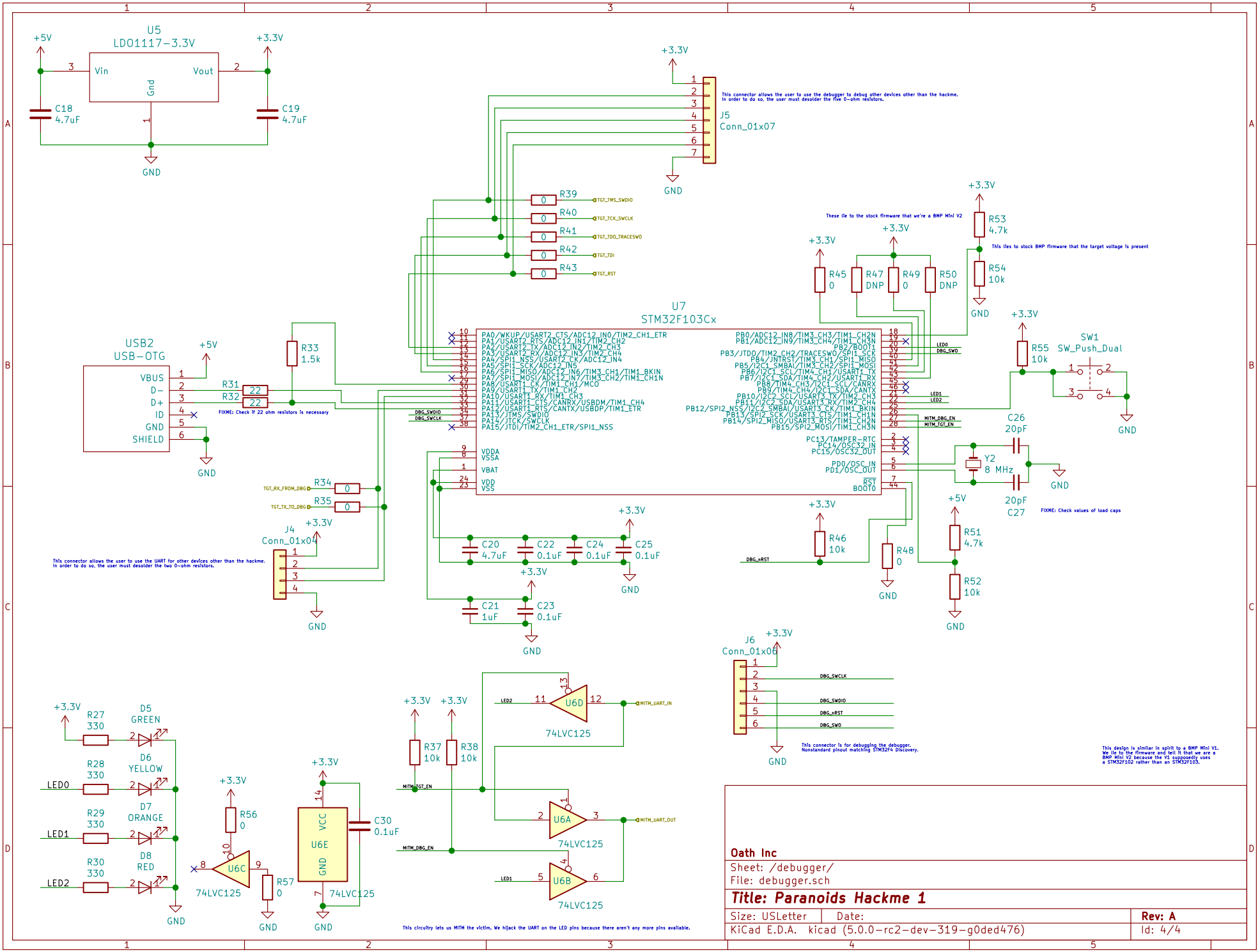
Oath Inc

Sheet: /target-cpld/

File: target-cpld.sch

Title: Paranoids Hackme 1

Size: USLetter	Date:	**Rev: A**
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)		Id: 3/4


U5
LDO1117-3.3V
Vin
Vout
Gnd
+5V
+3.3V
C18
4.7uF
C19
4.7uF
GND
J5
Conn_01x07
This connector allows the user to use the debugger to debug other devices other than the hackme. In order to do so, the user must desolder the five 0-ohm resistors.
R39
R40
R41
R42
R43
TGT_TMS_SWDIO
TGT_TCK_SWCLK
TGT_TDO_TRACESWO
TGT_TDI
TGT_RST
U7
STM32F103Cx
These lie to the stock firmware that we're a BMP Mini V2
R53
4.7k
R54
10k
This lies to stock BMP firmware that the target voltage is present
R45
0
R47
DNP
R49
0
R50
DNP
LED0
DBG_SWO
LED1
LED2
MITM_DBG_EN
MITM_TGT_EN
USB2
USB-OTG
VBUS
D-
D+
ID
GND
SHIELD
R31
22
R32
22
R33
1.5k
FIXME: Check if 22 ohm resistors is necessary
DBG_SWDIO
DBG_SWCLK
R55
10k
SW1
SW_Push_Dual
C26
20pF
Y2
8 MHz
20pF
C27
FIXME: Check values of load caps
R34
0
R35
0
TGT_RX_FROM_DBG
TGT_TX_TO_DBG
J4
Conn_01x04
This connector allows the user to use the UART for other devices other than the hackme. In order to do so, the user must desolder the two 0-ohm resistors.
C20
4.7uF
C22
0.1uF
C24
0.1uF
C25
0.1uF
C21
1uF
C23
0.1uF
R46
10k
DBG_nRST
R48
0
R51
4.7k
R52
10k
J6
Conn_01x06
DBG_SWCLK
DBG_SWDIO
DBG_nRST
DBG_SWO
This connector is for debugging the debugger. Nonstandard pinout matching STM32F4 Discovery.
This design is similar in spirit to a BMP Mini V1. We lie to the firmware and tell it that we are a BMP Mini V2 because the V1 supposedly uses a STM32F102 rather than an STM32F103.
R27
330
D5
GREEN
R28
330
D6
YELLOW
R29
330
D7
ORANGE
R30
330
D8
RED
LED0
LED1
LED2
R56
0
U6C
74LVC125
R57
0
U6E
VCC
GND
C30
0.1uF
74LVC125
R37
10k
R38
10k
MITM_TGT_EN
MITM_DBG_EN
U6D
U6A
U6B
MITM_UART_IN
MITM_UART_OUT
This circuitry lets us MITM the victim. We hijack the UART on the LED pins because there aren't any more pins available.
Oath Inc
Sheet: /debugger/
File: debugger.sch
Title: Paranoids Hackme 1
Size: USLetter
Date:
Rev: A
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)
Id: 4/4