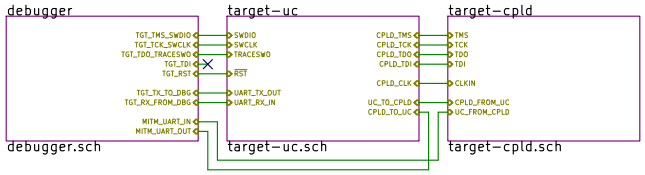


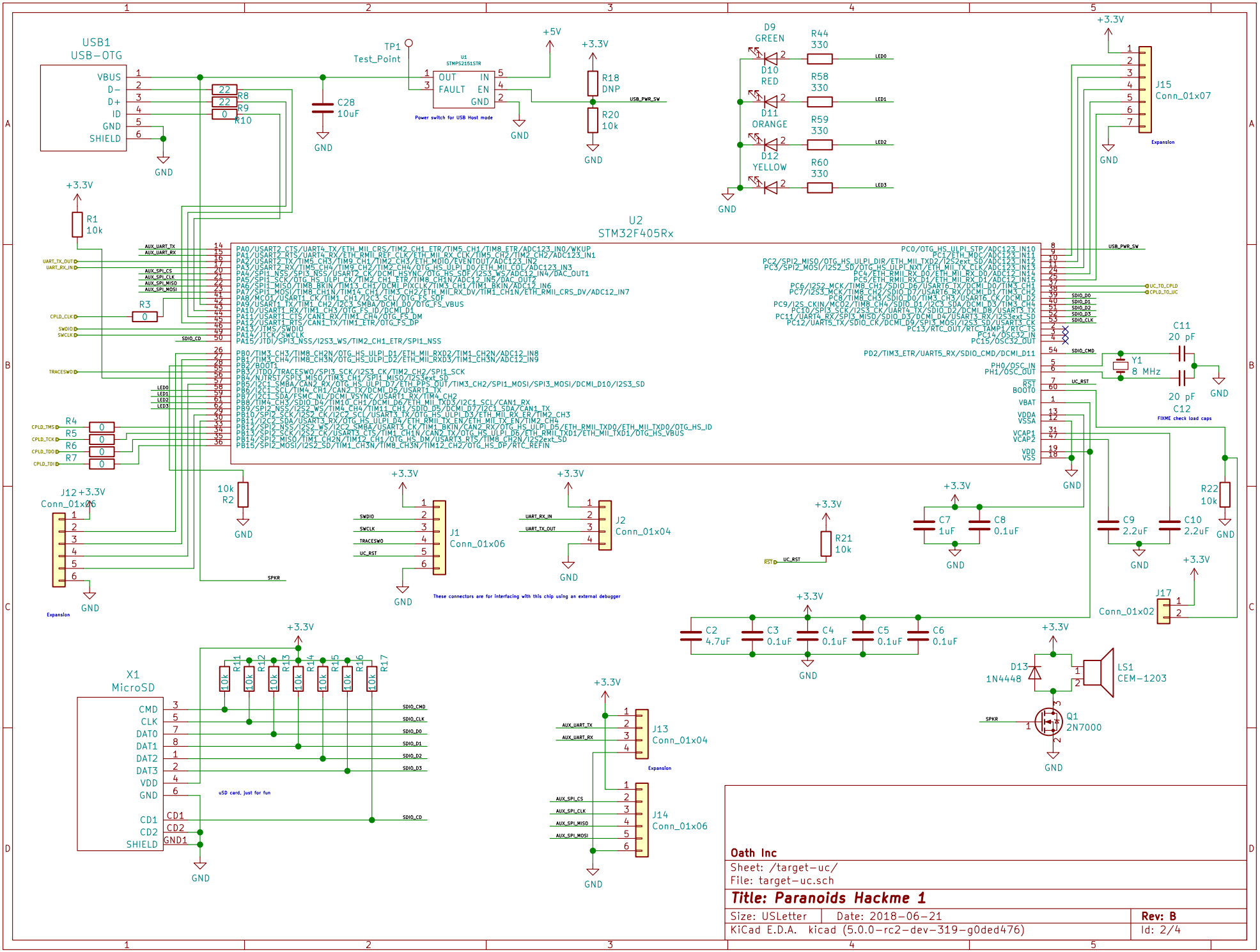
Oath Inc

Sheet: /

File: paranoids-hackme-1.sch

Title: Paranoids Hackme 1

Size: USLetter	Date: 2018-06-21	**Rev: B**
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)		Id: 1/4



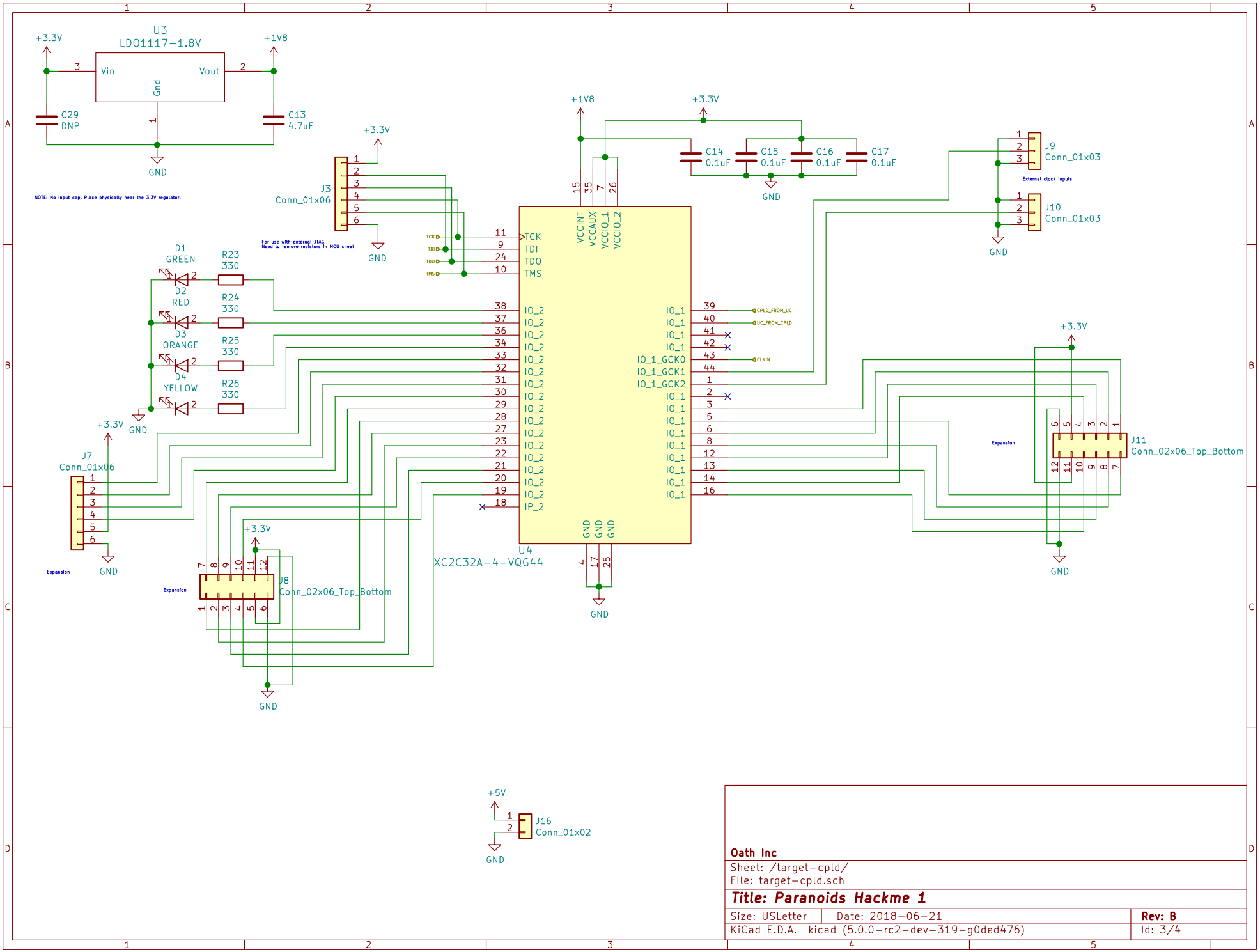
Oath Inc

Sheet: /target-uc/

File: target-uc.sch

Title: Paranoids Hackme 1

Size: USLetter	Date: 2018-06-21	**Rev: B**
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)		Id: 2/4



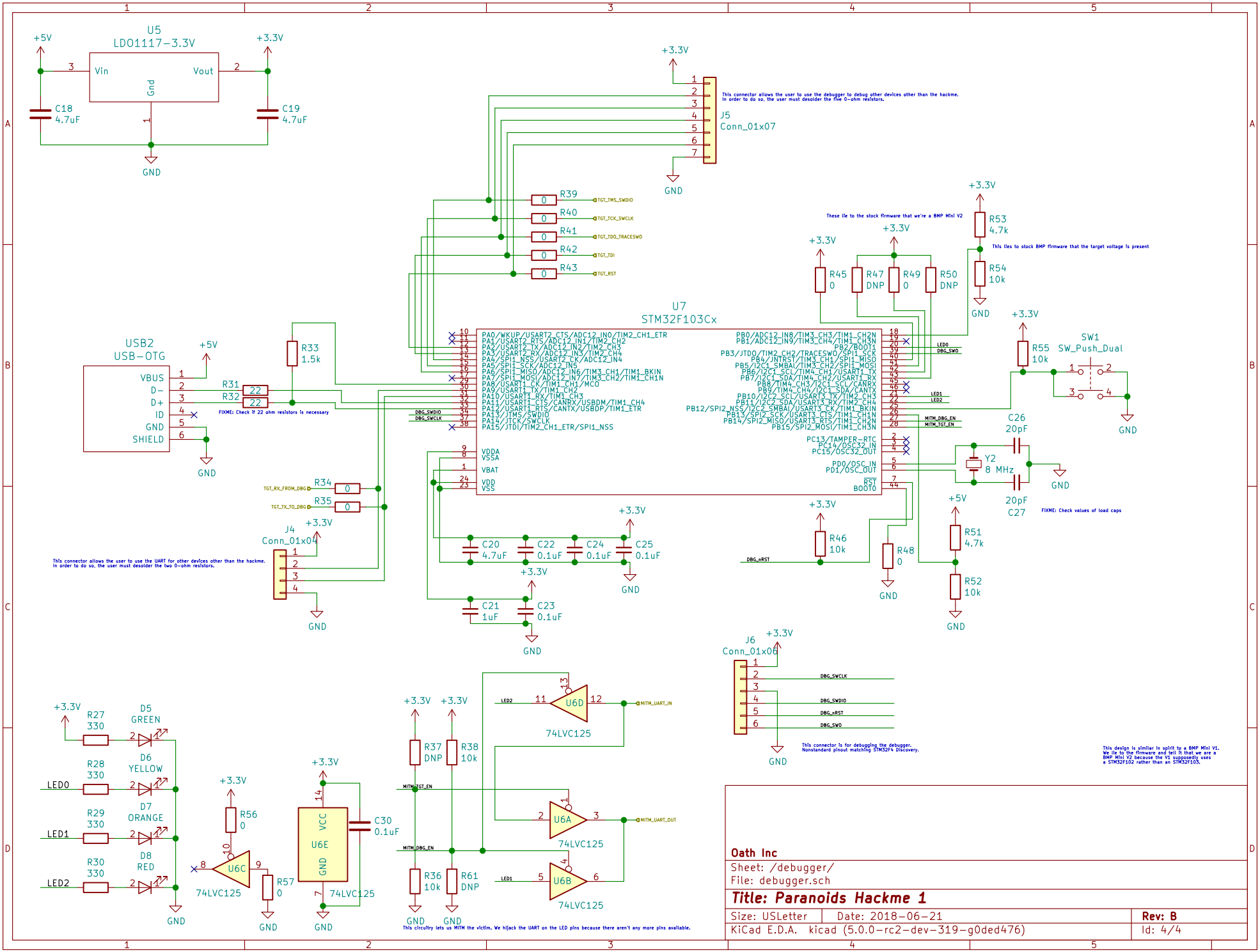
Oath Inc

Sheet: /target-cpld/

File: target-cpld.sch

Title: Paranoids Hackme 1

Size: USLetter	Date: 2018-06-21	**Rev: B**
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 tie to the stock firmware that we're a BMP Mini V2
R53
4.7k
R54
10k
This ties 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
R55
10k
SW1
SW_Push_Dual
C26
20pF
Y2
8 MHz
C27
20pF
FIXME: Check values of load caps
USB2
USB-OTG
VBUS
D-
D+
ID
GND
SHIELD
R31
22
R32
22
FIXME: Check if 22 ohm resistors is necessary
R33
1.5k
DBG_SWDIO
DBG_SWCLK
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
R37
DNP
R38
10k
R36
10k
R61
DNP
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: 2018-06-21
Rev: B
KiCad E.D.A. kicad (5.0.0-rc2-dev-319-g0ded476)
Id: 4/4