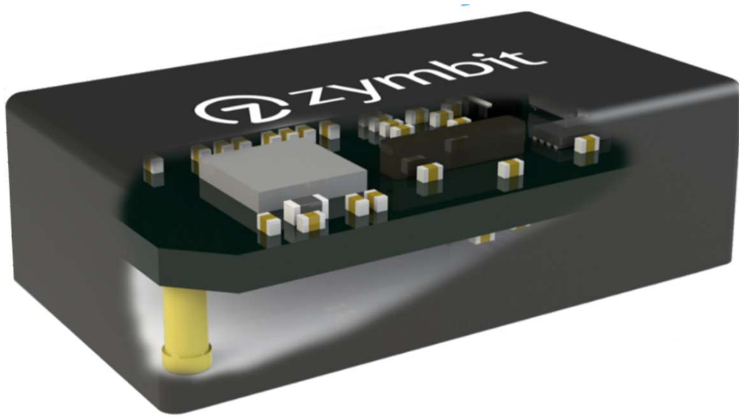
HSM4

Security Module for Embedded Computers

Hardware Datasheet Draft 0.2



Revision	Date	Description	Approved
0.1	10 May 2021	Initial Release	DR
0.2	14 May 2021	Updated Draft Release	DR

Contents

1. Overview

The HSM4 is a ‘snap in’ security module designed for easy integration within a secure manufacturing environment. The HSM4 has the following features:

- Fully encapsulated
- Single 30-pin connector
- Extended battery (external)
- Soft bind lock
- Measured identity
- Secure key storage and generation
- Cryptographic services
- Physical tamper sensors
- Manufacturing tools for high volume encryption & programming

2. HSM4 Pinout

The HSM4 uses the Hirose DF40HC(3.5)-30DS-0.4V(51) 30 pin, 0.4mm, 3.5mm mating height header. The customer PCB must use the Hirose **DF40C-30DP-0.4V(51)** 30 position connector. The HSM4 connector pinout is as follows for the customer side interface:

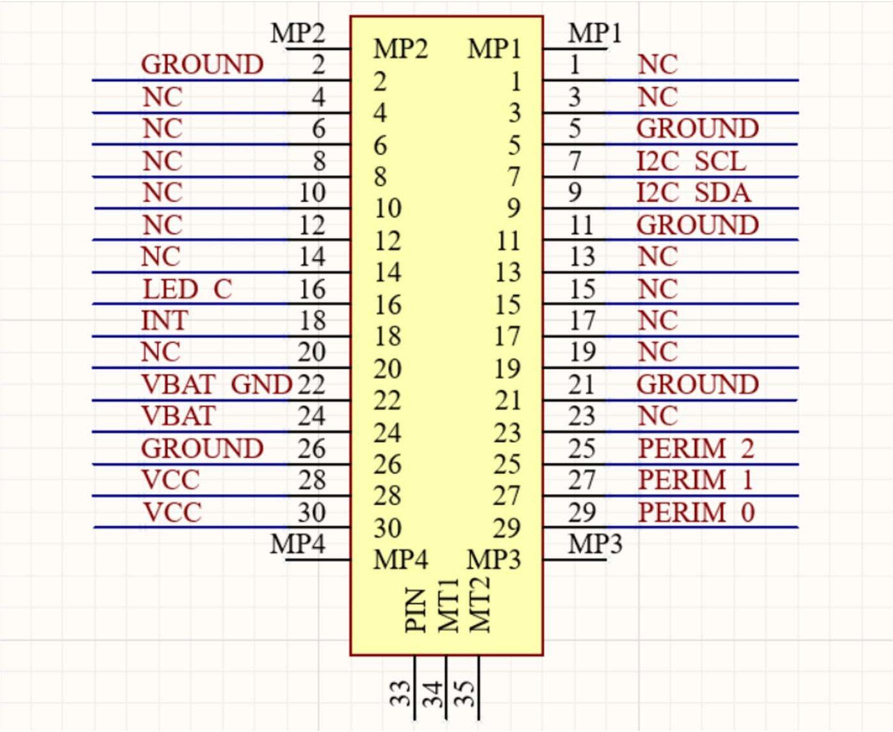


Figure 1 - HSM4 Pinout

Please note, the DF40C-30DP-0.4V(51) has 4 unconnected mounting pins in the corners which can be connected to a copper plane for mechanical strength or left unconnected as shown. Please see Mechanical below for proper orientation of the Hirose connector within the HSM4 enclosure footprint.

3. HSM4 Pin Descriptions

Pin Number	Pin Name	I/O	Description
1	N/C		No connect. Leave floating.
2	GROUND		Ground
3	N/C		No connect. Leave floating.
4	N/C		No connect. Leave floating.
5	GROUND		Ground
6	N/C		No connect. Leave floating.
7	I2C_SCL	I	I2C clock from SBC. For Raspberry Pi, this defaults to GPIO3.
8	N/C		No connect. Leave floating.
9	I2C_SDA	I/O	I2C data from SBC. For Raspberry Pi, this defaults to GPIO2.
10	N/C		No connect. Leave floating.
11	GROUND		Ground
12	N/C		No connect. Leave floating.
13	N/C		No connect. Leave floating.
14	N/C		No connect. Leave floating.
15	N/C		No connect. Leave floating.
16	LED_C	O	Led cathode. Connect to external LED cathode to monitor HSM4 status.
17	N/C		No connect. Leave floating.
18	INT	O	Transaction/Event interrupt to Pi. For Raspberry Pi, this defaults to GPIO4.
19	N/C		No connect. Leave floating.
20	N/C		No connect. Leave floating.
21	GROUND		Ground
22	VBAT_GND		Ground. Can be used as a dedicated battery ground or connect to system ground
23	N/C		No connect. Leave floating.
24	VBAT		Keep alive battery connection.
25	PERIM_2	I	Analog perimeter detect input channel 2
26	GROUND		Ground
27	PERIM_1	I	Analog perimeter detect input channel 1
28	VCC		Connect to Raspberry Pi 5.0V power supply.
29	PERIM_0	O	Analog perimeter detect pullup
30	VCC		Connect to Raspberry Pi 5.0V power supply.
MP1-MP4			Hirose DF40 mounting pads. Connect to copper pour or leave unconnected.
MT1-MT2			HSM4 mechanical mounting holes
PIN			HSM4 standoff mounting hole

4. HSM4 Mechanical Layout

Please see Hirose DF40 manual for recommended DF40C-30DP-0.4V(51) footprint.

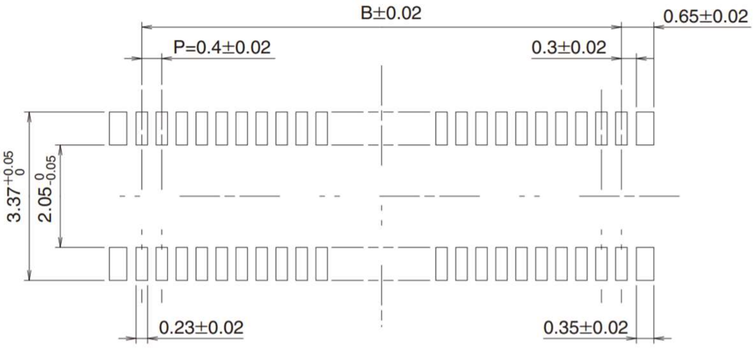


Figure 2 - DF40C-30DP-0.4V(51) footprint (B = 5.6mm)

https://www.hirose.com/en/product/document?clcode=CL0684-4033-4-51&productname=DF40C-100DS-0.4V(51)&series=DF40&documenttype=Catalog&lang=en&documentid=D31649_en

In addition to the 30 pin header, the HSM4 has 3 mechanical mounting points as well as the secure enclosure outline .

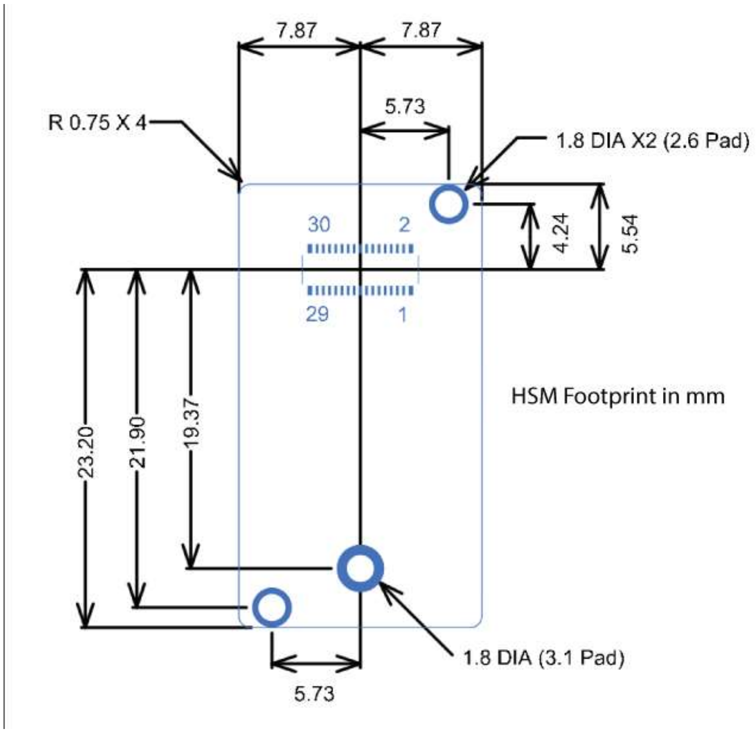


Figure 3 - HSM Footprint Dimensions, Top Down View (mm)

The two corner enclosure screws are M1.6-0.67 x 4 mm Type PT style thread forming screws https://www.fastenersuperstore.com/products/585834/thread-forming-screws?pid=18620

The center mechanical standoff screw is optional and is an M1.6 x 0.35mm thread, 4mm long pan head phillips screw.

https://www.mcmaster.com/92000A002/

5. HSM4 Power Supply

HSM4 is intended to be powered directly from the Raspberry Pi 5.0V supply rail. The HSM4 input tolerance is +/-0.5V and and consumes an average of 1.5uA during normal operation. Zymbit recommends adding 10uF and 0.1uF ceramic bypass capacitors to 5.0V near the HSM4 DF40 header VCC pins.

6. HSM4 Backup Battery

Backup battery is typically 3.0V lithium coin cell type. Zymbit uses CR2032, CR1025, etc depending on required capacity. The table below shows the theoretical estimated battery life calculated from capacity and average current consumption of the HSM4..

Battery	CR1025	CR2032	CR2
Battery Capacity (mAh)	30	200	850
Battery Life (Hours)	20,149	134,325	570,891
Battery Life (Days)	840	5,597	23,787
Battery Life (Years)	2.3	15.33	65.2

NOTE: Battery life assumes 100% powered from battery (no power to host), nominal temperature of 25C. While on battery power, the HSM4 will wake every 30 seconds to calibrate the RTC and every 1 second to check for perimeter detect faults.

7. Raspberry Pi I2C Best Practices

As the Raspberry Pi I2C bus drive strength can cause ringing in some applications, Zymbit recommends the addition of I2C series resistors to be added at the Pi header I2C pins. These can be populated with zero ohm resistors which can be adjusted if needed for I2C signal integrity. Zymbit does not recommend external I2C pullups on the HSM4 interface board.

8. LED

LED_C is driven by the HSM4 through a 470 ohm resistor which is onboard the HSM module. Connect external LED to a 3.3V power supply per image below. Zymbit uses ROHM SMLA13BC8TT86 blue LED.

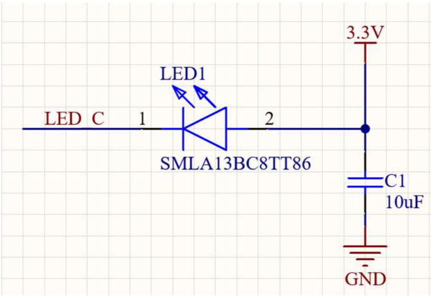


Figure 4 - HSM4 External LED Circuit for Customer PCB

9. Perimeter Detect

HSM4 perimeter detect consists of a pullup driver PERIM_0 and two perimeter input channels PERIM_1 and PERIM_2. A user can connect PERIM_1 or PERIM_2 through a wire, switch or flexible security blanket to PERIM_0 to create a physical tamper barrier.

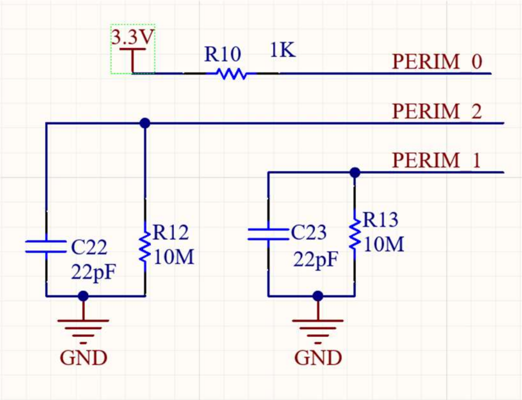


Figure 5 - HSM4 Perimeter Detect Onboard Circuitry (Do not add to customer board)

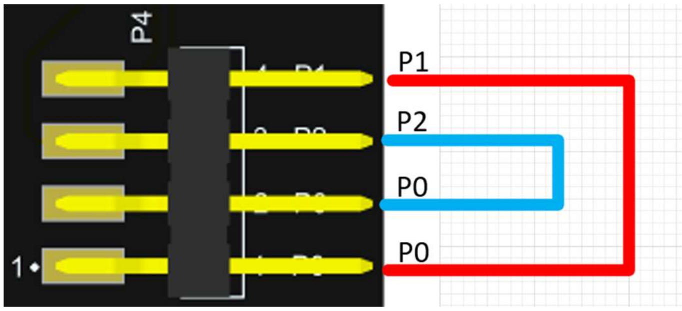


Figure 6 - Zymbit Recommended External Perimeter Detect Connections