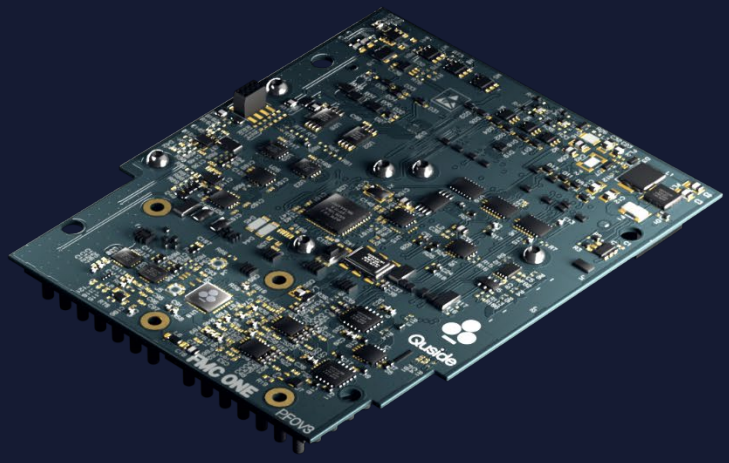
Quside

Product Datasheet

Quside Nellite™ Plus A41



The Quside Nellite™ Plus A41 is a **quantum entropy source** providing a direct interface with FPGA-based motherboards and is compliant to the FPGA Mezzanine Card (FMC) ANSI/ VITA 57.1 2019 standard connector. The device operates at 1 Gb/s with min-entropy bounds above 90%, and it is supplied with all the required firmware IP cores to operate, control, and interface the product with your motherboard.

Applications

Random numbers are required in a broad range of applications, including cybersecurity, high-performance computation, or gambling. The Quside Nellite™ Plus A41 is designed for high-performance quantum random generation for any FPGA product.

· Crypto-agile & quantum-safe deployments

· Quantum key distribution

· Post-quantum cryptography

· Advanced entropy monitoring

· Cloud security

· Entropy-as-a-Service

· High-performance Monte Carlo simulations

· Synthetic data generation

Features

· 1 Gb/s raw generation rates

· Above 90% quantum min-entropy bounds.

· Average min-entropy above 92%.
· Standard FMC interface (LPC/HPC) and FMC+

· Designed for FPGA developers.

· VHDL IP cores supplied for module control, monitoring and randomness extraction. Compatible with Xilinx FPGAs series 7000 and UltraScale.

· Compliant with NIST SP800B recommendations and passes DieHarder and NIST SP800-22 test suites.

· Metrology and monitoring of the entropy source and entropy quality

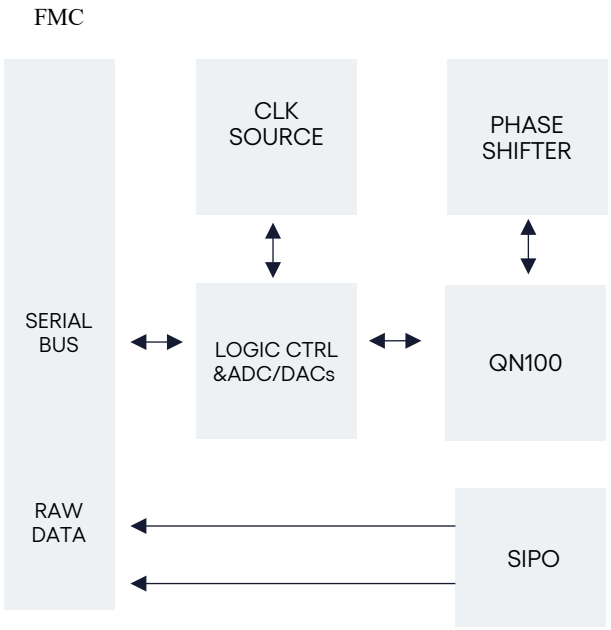


Figure 1. Block diagram of the Quside Nellite™ Plus A41.

Figure 1 shows a block diagram of the Quside Nellite™ Plus A41. The system consists of a randomness module card hosting the QN100, all in a compact mechanical case. The Quside Nellite™ Plus A41 card has an FMC port that allows for a smooth connection to an FPGA baseboard.

ELECTRICAL SPECIFICATIONS

	Units	Min	Typ	Max
Power consumption	W		5.0	

Status monitor SPECIFICATIONS

	Units	Min	Typ	Max
Bias monitor	mA	39	40	41
Temperature monitor[1] (T = environmental temp.)	°C	40	45	T + 20

RANDOMNESS SPECIFICATIONS

	Units	Min	Typ	Max
Quantum min-entropy[2]	Bits	0.9	0.92	
Raw bit rate	Mbps		1000	
Extracted bit rate[3]	Mbps		727	

ABSOLUTE MAXIMUM RATINGS

	Units	Min	Typ	Max
Operating Temperature[4]	°C	10	25	50
Storage Temperature	°C	0	25	80

FPGA RESOURCE USAGE ESTIMATION

	LTU	F/F	DSP	BRAM 36/18
Control IP Core	10163	13110	19.5	2
Randomness Extractor	2264	10324	256	4
Health Monitoring	4596	2052	0	1

[1] At T_{amb} = 25°C
[2] Quantum conditional min-entropy [R. Konig, R. Renner, & C. Schaffner (2009), IEEE Trans. Inf., *55*(9), 4337-4347] based on the physical model developed in [C. Abellán *et al.* (2015), Phys. Rev. Lett. (2015). *115*(25), 250403].
[3] Extraction from 352 bits to 256 bits, using the randomness extractor from [D. Frauchiger, R. Renner, & M. Troyer (2013), arXiv:1311.4547].
[4] Minimum value tested.

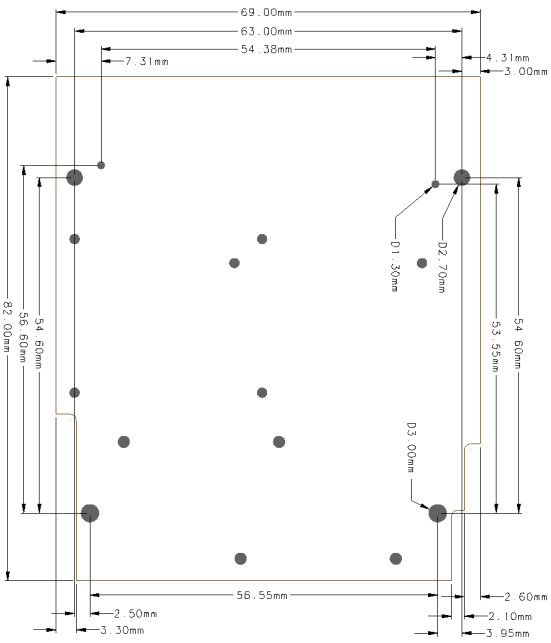
FMC CONNECTOR: ASP-134488-01					
Pin		NET	In/Out	Description	Level
C34	GA0	GA0	INPUT	EEPROM Address. GA0 connected to EEPROM GA1 following ANSI.VITA57	3.3V
C31	SDA	IPMI_SDA	INPUT	I2C bus for IPMI protocol	3.3V
C30	SCL	IPMI_SCL	BI	I2C bus for IPMI protocol	3.3V
C26	LA27_P	FPGA_NRST	INPUT	Reset signal for the Microcontroller	VADJ*
C23	LA18_N_CC	FPGA_IO4	INPUT/OUTPUT	GPIO Between FPGA&uC	VADJ*
C22	LA18_P_CC	FPGA_IO3	INPUT/OUTPUT	GPIO Between FPGA&uC	VADJ*
C19	LA14_N	FPGA_IO2	INPUT/OUTPUT	GPIO Between FPGA&uC	VADJ*
C18	LA14_P	FPGA_IO1	INPUT/OUTPUT	GPIO Between FPGA&uC	VADJ*
C15	LA10_N	FPGA_IO0	INPUT/OUTPUT	GPIO Between FPGA&uC	VADJ*
D35	GA1	GA1	INPUT	EEPROM Address. GA1 connected to EEPROM GA0 following ANSI.VITA57	3.3V
D24	LA23_N	RAW_FPGA-A_N	OUTPUT	Output raw data (1 GHZ)	LVDS
D23	LA23_P	RAW_FPGA-A_P	OUTPUT	Output raw data (1 GHZ)	LVDS
D9	LA01_N_CC	FPGA_USART-RX	INPUT	FPGA&uC Serial port RX	VADJ*
D8	LA01_P_CC	FPGA_USART-TX	OUTPUT	FPGA&uC Serial port TX	VADJ*
G10	LA03_N	SPI1_MISO	OUT PUT	FPGA&Uc SPI port pins	VADJ*
G9	LA03_P	SPI1_MOSI	INPUT	FPGA&Uc SPI port pins	VADJ*
G7	LA00_N_CC	SPI1_SCK	INPUT	FPGA&Uc SPI port pins	VADJ*
G6	LA00_P_CC	SPI1_NSS	INPUT	FPGA&Uc SPI port pins	VADJ*
G3	CLK1_M2C_N	CLK_REC_SIPO_N	OUTPUT	Output SIPO clock	LVDS
G2	CLK1_M2C_P	CLK_REC_SIPO_P	OUTPUT	Output SIPO clock	LVDS
H14	LA07_N	DATA_OUT-2_N	OUTPUT	SIPO output data	LVDS
H13	LA07_P	DATA_OUT-2_P	OUTPUT	SIPO output data	LVDS
H8	LA02_N	DATA_OUT-1_N	OUTPUT	SIPO output data	LVDS
H7	LA02_P	DATA_OUT-1_P	OUTPUT	SIPO output data	LVDS
H5	CLK0_M2C_N	CLK_REC_N	OUTPUT	OUTPUT clock	LVDS
H4	CLK0_M2C_P	CLK_REC_P	OUTPUT	OUTPUT clock	LVDS

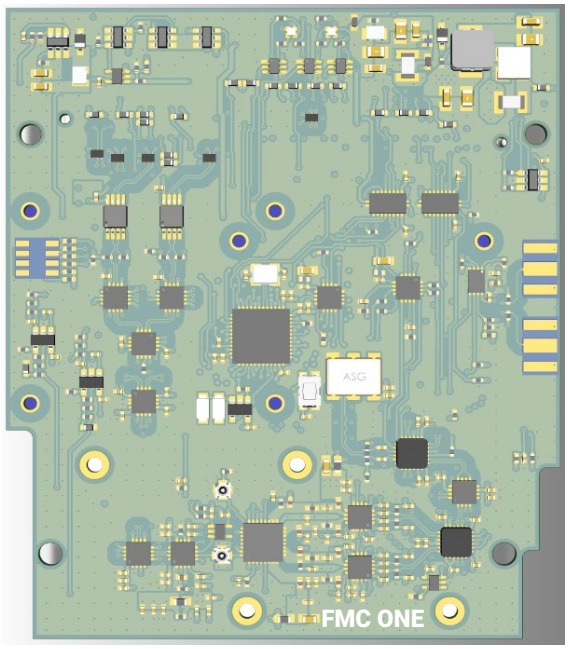
FMC PIN CONFIGURATION

Mechanical Specifications

The Quside Nellite™ Plus A41 has been designed fulfilling the ANSI/ VITA 57.1 2019 standard.

The module dimensions are 82 x 69 mm^2 and four mounting holes sized for an M2.5 screw.





Thanks for being part of our quantum journey!