वर्गीय आवश्यकताओं के लिए मानक

टीईसी ९१०२०:२०२५

STANDARD FOR GENERIC REQUIREMENTS

TEC 91020:2024

क्वांटम यादृच्छिक संख्या जनरेटर

Quantum Random Number Generator

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 1: October, 2024

FOREWORD

Telecommunication Engineering Centre (TEC) functions under the Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centres (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

Random Number Generators (RNG) produce sequences of random numbers which are essential for a number of applications: encrypted data transmission using random numbers as secret keys, key vaults, gaming, Quantum Key Distribution, etc. Quantum Random Number Generator (QRNG) generates random numbers with a high source of entropy by exploiting the properties of quantum physics. This document describes the generic requirements and specifications for Quantum Random Number Generator including the functional architecture for the quantum entropy source.

CONTENTS

Clause Particulars Page No.

HISTORY SHEET

Sl. No.	Standard/ Document No.	Title	Remarks
1.	TEC 91020:2024	Standard for Generic Requirements (GR) of Quantum Random Number Generator	Release 1

REFERENCES

S.No.	*Document No.*	*Title*
1.	ITU-T X.1702	Quantum noise random number generator architecture
2.	NIST SP 800-90A Rev. 1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
3.	NIST SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation
4.	NIST SP 800-90C	Recommendation for Random Bit Generator (RBG) Constructions
5.	NIST SP 800-22 Rev. 1	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
6.	IS/ISO/IEC 18031 : 2011	Specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model
7.	TEC 11016:2016	Electromagnetic Compatibility Standard for Telecommunication Equipment
8.	ISO 9001:2015	Quality management system
9.	IEC 60825-1	Safety of laser products - Part 1: Equipment classification and requirements

10.	IEC 60825-2	Safety of laser products - Part 2: Safety of optical fibre communication systems (OFCSs)
11.	CISPR 32:2015+A1:2019	Electromagnetic compatibility of multimedia equipment - Emission requirements
12.	CISPR 11 {2024}	Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement
13.	IEC 61000-4-2 {2008}	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test
14.	IEC 61000-4-3 (2020)	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test
15.	IEC 61000- 4- 4 {2012}	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test
16.	IEC 61000-4-5 (2014)	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
17.	IEC 61000-4-6 (2023)	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields

18.	IEC 61000-4-11 (2020)	Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests
19.	IEC 61000-4-29:2000	Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests
20.	IS/IEC 62368-1:2023	Audio/video, information and communication technology equipment - Part 1: Safety requirements

Note:

Unless otherwise explicitly stated, the latest approved issue of the documents referred to above, with all amendments in force, on the issuance date of this GR shall be applicable.

CHAPTER-1

Technical Requirements

1.1 Introduction to Quantum Random Number Generator

1.1.1 This document describes the generic requirements and specifications for Quantum Random Number Generator.

1.1.2 Random number generators (RNGs) are crucial in many fields, particularly in cryptography, where it is essential for generating secure encryption and decryption keys. Predictable random numbers can lead to potential backdoor attacks, compromising security. It is, therefore, imperative to use a high entropy source RNG, based on quantum phenomenon, to generate true random numbers. Unlike classical processes, quantum processes are fundamentally unpredictable, making the numbers generated from a quantum source intrinsically random and non-deterministic.

1.1.3 Properties of Random Number Generator

(i) **Uniformity:** There should be equal probability for the occurrence of 0's and 1's at any point of random sequence generation i.e. the expected number of 0's and 1's in the sequence should be equal.

(ii) **Scalability:** The randomness should be retained for any sub-sequences extracted randomly from the generated sequence.

(iii) **Consistency**: The random number generator should behave consistently regardless of the input or time.

(iv) **Forward secrecy:** It refers to the inability to predict future output of the RNG based on the knowledge of previous output values and/or internal states.

(v) **Backward secrecy:** It refers to the inability to determine prior output of an RNG, given knowledge of the current or any future output of the RNG.

(vi) **Stability:** It refers to the ability to produce a stable random sequence over a long period, without being disturbed by the environment.

1.2 Classification of Random Number Generators

The Random Number Generators can be classified into the following types:

1.2.1 **Pseudo Random Number Generators (PRNG):** Pseudo Random Number Generators, also known as Deterministic Random Bit Generator (DRBG), use algorithms or mathematical functions to produce sequences of random numbers. PRNGs generate a sequence of numbers that approximate the properties of random numbers. A PRNG starts from an arbitrary starting state using an initial seed. PRNGs can generate random numbers at high speeds, however, they have the disadvantage of being reproducible if the seed is known.

1.2.2 **Physical True Random Number Generators (PTRNG):** PTRNGs produce high entropy random numbers from a physical noise source based on a randomness-exhibiting physical phenomenon. This phenomenon may be realized by a physical experiment or by an electronic circuit.

1.2.3 **Non-Physical True Random Number Generators (NPTRNG):** NPTRNGs generate 'true' random numbers, but unlike PTRNGs they do not employ dedicated hardware designs or physical experiments as noise sources. Instead, NPTRNGs prevalently exploit non-physical noise sources such as system data (timing values, RAM data, etc.) or human interaction (key board and mouse events, etc).

1.2.4 Based on the phenomenon used, True Random Number Generators can be classified as:

(i) **Classical TRNG:** These rely on classical physics phenomena such as Raman scattering, Clock Jitter, etc. to generate random numbers. The chaotic source of classical randomness is susceptible to initial conditions and thus, could be exploited.

(ii) **Quantum Random Number Generator (QRNG):** QRNG generates random numbers using the principles of quantum physics. Unlike PRNGs which rely on deterministic algorithms and classical TRNGs which depend on chaotic physical phenomena, QRNGs leverage the inherent randomness of quantum phenomena. These devices typically utilize properties like the uncertainty principle, superposition, entanglement, etc. to produce unpredictable sequences of numbers.

1.3 Fundamental Sources of Quantum Randomness

1.3.1 Quantum physics provides randomness with inherent unpredictability by exploiting the fundamental indeterminism of quantum experiments.

1.3.2 The quantum phenomena include quantum state superposition, quantum state entanglement, Heisenberg uncertainty, quantum tunnelling, spontaneous emission or radioactive decay, etc. The quantum phenomena used for random number generation may be classified as:

(i) Optical Quantum Phenomenon:

- Branching path, eg. photons from a single photon source or photons from an anti-bunched or sub-Poissonian source passed through a semi-transparent mirror or beam splitter.
- Time of arrival of photons
- Amplified spontaneous emission
- Photon counting
- Phase noise of a single-mode laser
- Spontaneous parametric down-conversion leading to binary phase state selection in a degenerate optical parametric oscillator.
- Fluctuations in vacuum energy measured through homodyne detection.
- EPR Entanglement of field quadratures of multi-mode squeezed light generated by spontaneous four wave mixing (SFWM) and/or spontaneous down conversion (SPDC)
- Any other methods using Optical Quantum phenomena, not covered above.

(ii) Non-Optical Quantum Phenomenon:

- Shot noise, a quantum mechanical noise source in electronic circuits.
- Spin noise in atomic systems.
- Radioactive decay.
- Quantum Tunnelling eg. amplification of the signal produced on the base of a reverse-biased transistor. The emitter is saturated with

electrons and occasionally they will tunnel through the bandgap and exit via the base.

- Quantum Interference, where the probability amplitude of different quantum states superpose, leading to redistribution of probability density.
- Any other methods using Quantum phenomena, not covered above.

1.4 Applications of QRNG

1.4.1 **Quantum-secure Cryptography**: Random numbers are crucial for creating secure cryptographic keys. QRNGs can be used to generate truly random numbers that can be used to create unbreakable cryptographic keys for secure communication.

1.4.2 **V2X Security:** QRNG can be used to secure vehicle-to-everything (V2X) communications, ensuring the privacy and safety of connected vehicles.

1.4.3 **Online Gaming:** Random numbers are essential in the gaming industry for creating fair and unbiased games. QRNGs can be used to generate truly random numbers for games such as lotteries, online casinos, and other gambling applications.

1.4.4 **Mobile Phones:** With QRNG chip embedded in mobile phone, enhanced security can be applied to any service and any app on the phone. The QRNG chip adds an additional layer of authentication, boosting security by generating truly unpredictable and random numbers that are used for encryption.

1.4.5 **Telecommunications:** QRNGs can be used in LTE/5G authentication centre (AuC) and other network functions to ensure quantum-safe security.

1.4.6 **Data Centres:** QRNGs can be used for securing data at rest in data centers by providing a source of true randomness for cryptographic operations. This can be used to generate strong encryption keys, randomize data, and create unique identifiers for data elements.

1.4.7 **Tokenization:** Tokenization is crucial for securing and masking customer data, especially in the banking sector. With the rise in digital adoption, the demand for tokens has increased, leading to repetition and correlation in token generation. QRNG can be used to generate random tokens.

1.4.8 **Exams and Certifications:** QRNG can be used to generate unique identifiers and randomize exam questions, preventing cheating and ensuring fairness.

1.4.9 **Simulation and Modelling**: In many scientific applications, truly random numbers are needed to simulate natural phenomena, such as the weather, the behavior of materials, and biological systems. QRNGs can provide a source of truly random numbers for these simulations

1.4.10 **Statistical analysis:** Random numbers are essential in statistical analysis, for example, in Monte Carlo simulations, where random numbers are used to generate samples for statistical analysis. QRNGs can provide a source of truly random numbers for these types of applications.

1.5 Types of QRNG

1.5.1 The QRNG can be offered in various form factors, categorized as below:

(i) Category A: *Network Appliance QRNG*

It is a network-attached device, which securely generates and delivers high-quality random numbers for security and cryptographic applications in enterprise, government, gaming, data centers and cloud environments. It can be inserted in, or removed from, an operating network with no impact on any other appliance, such as servers, switches, encryptors, authentication servers and any other security modules. It can be used a randomness source in cloud or distributed environments, providing secure keys for Virtual Machines (VMs), Virtual Private Networks (VPNs), and remote desktops. It can also be used in Randomness-as-a-Service (RaaS) environments.

(ii) Category B: *Portable QRNG with USB interface*

It is a portable USB device that can be directly connected via USB port, offering convenient and portable random number generation capabilities. It can be used by applications for securing sensitive data and online transactions.

(iii) Category C: QRNG with *PCIe interface*

It is a QRNG with PCIe (peripheral component interconnect express) interface used for integrating into various applications/systems. It provides true random numbers to applications, servers, and key management systems to support data protection, numerical, simulations, gaming and other uses.

(iv) Category D: *Chip-based QRNG*

It is a QRNG integrated in a miniaturized semiconductor/photonic integrated circuit chip/Planar lightwave circuit which can be directly embedded into various cryptographic modules used in various systems. It can be used in mobile handsets, IoT, edge devices, etc.

1.6 Functional Architecture of Quantum Entropy Source

1.6.1 In random number generation, ensuring true randomness is crucial for security, reliability, and fairness in various applications like cryptography, simulations, and gaming. Quantum entropy sources provide randomness based on natural phenomena that are inherently unpredictable. Unlike pseudo-random algorithms, which are deterministic and potentially vulnerable to prediction, quantum entropy sources offer randomness that resists cryptographic attacks and ensures unbiased outcomes. It enhances the integrity and trustworthiness of systems dependent on random number generation.

1.6.2 The high-level block diagram for the entropy source in True Random Number Generator can be represented as below:

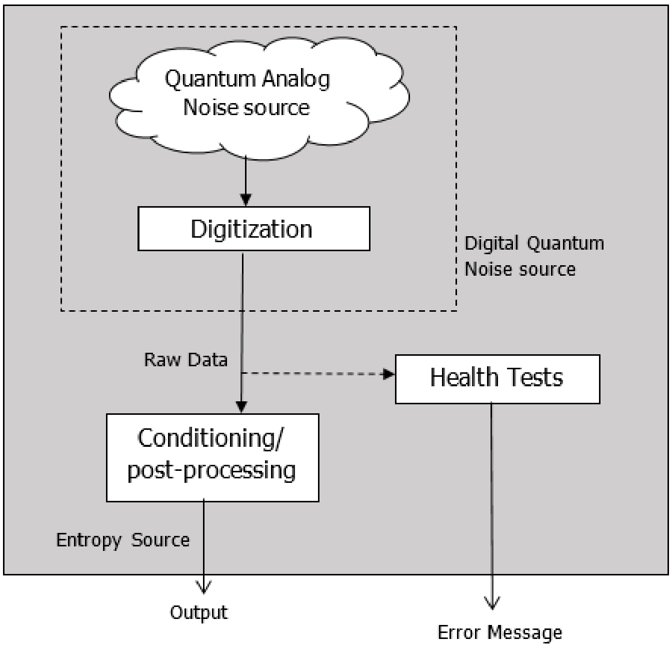
Quantum Analog Noise source
Digitization
Digital Quantum Noise source
Raw Data
Health Tests
Conditioning/ post-processing
Entropy Source
Output
Error Message

Figure 1: High-Level Block Diagram of Quantum Entropy Source

(i) Noise Source: The noise source is the root of security for the entropy source and for the Random Number Generator as a whole. This is the component that contains the non-deterministic, entropy-providing process that is ultimately responsible for the uncertainty associated with the random numbers output by the entropy source. If the non-deterministic activity being sampled produces something other than binary data, the sampling process includes a digitization process that converts the output samples to bits. The output of the digitized noise source is called the raw data.

(ii) Conditioning Component / Post-processing: The optional conditioning component or post-processing is a deterministic function responsible for reducing bias and/or increasing the entropy rate of the resulting output bits (if necessary to obtain a target value).

(iii) Health tests: Health Tests are an integral part of the entropy source design that are intended to ensure that the noise source and the entire entropy source continue to operate as expected. When testing the entropy source, the end goal is to obtain assurance that failures of the entropy source are caught quickly and with a high probability. Another aspect of health testing strategy is determining the likely failure modes for the entropy source and, in particular, for the noise source. Health tests are expected to include tests that can detect failure conditions which may include insufficient entropy generation, environmental instability, hardware malfunctions, external interferences, etc.

1.6.3 The functional architecture of Quantum Entropy sources in QRNG shall be as per ITU-T Recommendation X.1702 "*Quantum noise random number generator architecture*".

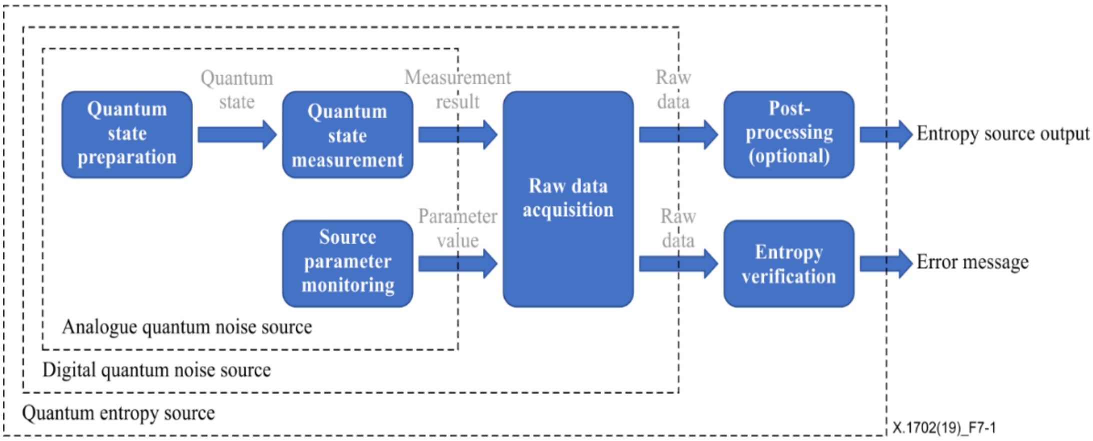

Figure 2: Functional architecture of a quantum entropy source

[Reference: ITU-T X.1072]

1.6.4 A quantum process to generate quantum noise can be decomposed in two steps: a quantum state preparation and a quantum state measurement. The generation of raw data by the Quantum Entropy Source shall include the following functional modules:

(i) **Quantum state preparation:** The quantum state can be optical or non-optical and either remain the same or be different in each iteration. The preparation can be active or passive;

(ii) **Quantum state measurement:** Applying a measurement basis to the propagated state or the state derived from the quantum state preparation. This measurement basis can either remain the same or be different from one measurement to another.

NOTE – The combination of the 'quantum state preparation' module and the 'quantum state measurement' module composes an analogue quantum noise source.

(iii) **Raw data acquisition:** This step is to generate raw data from quantum state measurement results. A digitization step is needed if the quantum state measurement results are analogue. The raw data acquisition module outputs the raw data that will be used to generate the digital quantum noise source output.

(iv) **Post-processing/ Randomness Extractor (optional):** In some cases, the raw data might be post-processed before being output as entropy source output. One of the main reasons is most QRNG sources output is a mixture of both classical and quantum noise. Therefore, the output requires post-processing to distill quantum randomness and also to increase the entropy content of each bit of the entropy source output.

Depending on the number of functional steps used for the description of the quantum entropy source, the entropy source can output either the raw data generated by the 'raw data acquisition' step, or the output from the 'post-processing' step

1.6.5 The entropy estimation of quantum noise sources is based on ideal models that are difficult to implement perfectly. In most cases, the entropy of a quantum noise source is partly due to the relevant quantum process and some additional physical noise coming from implementation imperfections. It is possible for most quantum noise sources to estimate the entropy solely due to the relevant quantum process.

1.6.6 Quantum entropy sources can be classified in two subclasses depending on their means of entropy estimation. One subclass of quantum entropy source will assess a given minimum entropy amount by measuring the implementation imperfections and verifying that they are within defined acceptable value ranges. This subclass of quantum entropy sources (QESs) is called QES1. Another subclass of QESs, called QES2, will directly assess their entropy amount by measuring signatures of the quantum process. Then, in both cases, by using an appropriate randomness extractor, it is possible to create an output whose entropy arises solely from the considered quantum process.

1.6.7 The description of a quantum entropy source shall include the definitions of the conditions (e.g., environmental constraints) under which this description remains valid.

(i) In the case of QES1 sources, these conditions are required to include at least:

— the noise arising from implementation imperfections; and

— the range over which the value of this noise can vary

(ii) In the case of QES2 sources, these conditions are required to include at least:

— the signature(s) of the quantum process; and

— their acceptance range used to assess the entropy of the quantum source under evaluation and to ensure the continued working of the components of the system.

1.6.8 The description of the quantum state preparation and measurement modules is required to rely on quantum formalism.

1.6.9 A method of estimation of the entropy generated by the quantum entropy source under evaluation is required to be based on the description of the source. This estimation is recommended to be based on quantum information theory or other approved methods related to quantum physics.

1.6.10 **Entropy Assessment:** The QRNG shall carry out the assessment of the entropy generated by the Quantum process and carried by the raw data by a three-step process as below:

(i) **Source parameter monitoring:** A source parameter monitoring function is required to monitor the conditions under which the raw data is generated by the digital entropy source. The source parameters are acquired by this function to be used as inputs for the verification of the entropy of the raw data;

— In the case of QES1 entropy sources, the monitoring function is required to monitor all the conditions listed in the description of the quantum entropy source that impact the entropy value of this source (e.g., noise arising from implementation imperfections and external conditions).

— In the case of QES2 entropy sources, the monitoring function is required to estimate the signature(s) of the quantum process and to compare them with their acceptance ranges defined in the description in order to assess the entropy of the source and to ensure components of the system are operating within acceptable parameters where required by the description.

(ii) **Raw data acquisition:** The source parameters are digitized and added in the flow of raw data. These source parameters will not be used to generate the output flow of the entropy source but to verify its entropy.

Note: The raw data is composed of the bit sequence ('measurement result') and additional digital values ('parameter value', e.g., temperature, voltage, tampering attempts etc.) generated by the entropy source.

(iii) **Entropy verification:** The raw data will be processed in order to verify if the entropy generated by the digital quantum noise source is at least higher than the minimum entropy amount specified. If this is not the case, an **error message** may be generated by the 'entropy verification' module and output from the quantum entropy source.

1.7 Requirements for Quantum Entropy Source

1.7.1 The entire design of the Quantum entropy source shall be documented, including the interaction among the various components. The documentation shall justify why the Quantum entropy source can be relied upon to produce bits with sufficient entropy.

1.7.2 Documentation shall describe the operation of the Quantum entropy source, including how the Quantum entropy source works, and how to obtain data from within the Quantum entropy source for validation testing,

1.7.3 Documentation shall describe the range of operating conditions (e.g., temperature range, voltages, system activity, etc.) under which the Quantum entropy source is claimed to operate correctly. The Quantum entropy source outputs are expected to have similar entropy rates in this specified range of operating conditions.

1.7.4 The Quantum entropy source shall have a well-defined (conceptual) security boundary. This security boundary shall be documented; the documentation shall include a description of the content of the security boundary.

1.7.5 When a post-processing component is not used, the output from the Quantum entropy source is the output of the noise source, and no additional interface is required. In this case, the Quantum noise source output is available during both validation, testing and normal operation.

1.7.6 When a post-processing component is included in the Quantum entropy source, the output from the Quantum entropy source is the output of the post-processing component, and an interface is required to access the quantum noise-source output. In this case, the quantum noise-source output shall be accessible via the interface during validation testing, but the interface may be disabled otherwise. The manufacturer shall fully document the method used to get access to the raw Quantum noise source samples. If the noise-source interface is not disabled during normal operation, any noise-source output using this interface shall not be provided to the post-processing component for processing and eventual output as normal Quantum entropy-source output.

1.7.7 The Quantum entropy source may restrict access to raw quantum noise source samples to special circumstances that are not available to users in the field, and the documentation shall explain why this restriction is not expected to substantially alter the behaviour of the Quantum entropy source as tested during validation.

1.7.8 Documentation shall contain a description of the restarting process applied during the restart tests.

1.7.9 Documentation shall contain a concrete information theoretical randomness proof using entropic uncertainty relation, universal hash lemma or non-classical inequality, etc.

1.8 Requirements for Quantum Noise Source

1.8.1 The operation of the Quantum noise source shall be documented; this documentation shall include a description of how the Quantum noise source works, where the unpredictability comes from, and rationale for why the Quantum noise source provides acceptable entropy output, basis of randomness and should reference relevant, existing research and literature.

1.8.2 The behaviour of the Quantum noise source shall be stationary (i.e., the probability distributions of the Quantum noise source outputs do not change when shifted in time). Documentation shall include why it is believed that the entropy rate does not change significantly during normal operation. This can be in broad terms of where the unpredictability comes from and a rough description of the behaviour of the Quantum noise source (to show that it is reasonable to assume that the behaviour is stationary).

1.8.3 Documentation shall provide an explicit statement of the expected entropy provided by the Quantum noise source outputs and provide a technical argument for why the noise source can support that entropy rate. To support this, documentation may include a stochastic model of the Quantum noise source outputs, and an entropy estimation based on this stochastic model may be included.

1.8.4 The Quantum noise source state shall be protected from adversarial knowledge or influence to the greatest extent possible. The methods used for this shall be documented, including a description of the (conceptual) security boundary's role in protecting the Quantum noise source from adversarial observation or influence.

1.8.5 Although the Quantum noise source is not required to produce unbiased and independent outputs, it shall exhibit random behaviour; i.e., the output shall not be definable by any known algorithmic rule. Documentation shall indicate whether the noise source produces IID data or non-IID data. If the manufacturer makes an IID claim, documentation shall include rationale for the claim.

1.8.6 The Quantum noise source shall generate fixed-length bitstrings. A description of the output space of the Quantum noise source shall be provided. Documentation shall specify the fixed symbol size (in bits) and the list (or range) of all possible outputs from the quantum noise source.

1.8.7 An additional noise source may be included if the primary entropy source is insufficiently reliable from a failure perspective. In this case, the additional entropy source shall satisfy the same requirements as the primary noise source.

1.8.8 If additional noise source outputs to increase security are used, a document that describes the additional noise sources shall be included.

1.9 Requirements for the Post-processing

1.9.1 The manufacturer shall document which post-processing (conditioning) component is used and the details about its implementation (e.g., the hash function, cryptographic algorithms, and/or key size used). Documentation shall also include the input and the output sizes ,n_{in} and n_{out} of the post-processing component.

1.9.2 The documentation shall describe how the post-processing component enhances the entropy obtained from the QRNG, ensuring that the output data meets randomness and security standards.

1.9.3 If the post-processing component uses cryptographic keys, the keys may be (1) fixed to a predetermined value, (2) set using some additional input to the device, or (3) generated by using the quantum noise source outputs. The key shall be determined before any outputs are generated from the post-processing component.

1.9.4 Any value which is used to determine the key shall not be used as any other input to the post-processing component. The input entropy to the post-processing component (h_{in}) shall not include any entropy provided to the key of a keyed function.

1.9.5 For Quantum entropy sources containing a post-processing component that is not specified in NIST SP 800-90B, a description of the post-processing component shall be provided. Documentation shall state the narrowest internal width and the size of the output blocks from the post-processing component. The manufacturer shall provide mathematical evidence that the post-processing component is suitable to be used to condition the Quantum noise source output, and does not significantly reduce the entropy rate of the entropy source output. The manufacturer shall also provide a justification about why the post-processing component does not act poorly when the noise source data is not independent.

1.9.6 The post-processing component shall not extend the raw data it receives as input.

1.9.7 The post-processing component, also known as the randomness extractor used to increase the entropy per bit of the source is recommended to be a quantum-proof extractor (optional).

1.10 Requirements for Health Tests

1.10.1 The health testing of Quantum noise sources shall be done to detect failures of the noise source, based on the expected output during a failure, or to detect a deviation from the expected output during the normal operation of the Quantum noise source. Health tests are expected to raise an alarm,

(i) When there is a significant decrease in the entropy of the outputs,

(ii) When Quantum noise source failure occurs, or

(iii) When hardware fails, and implementations do not work correctly.

1.10.2 Health Tests shall be applied to the outputs of a Quantum noise source before any post-processing is done.

1.10.3 Start-up health tests are designed to be performed after powering up, or rebooting, and before the first use of the Quantum entropy source. The

start-up test shall be applied immediately after the QRNG has been started. It shall detect a total failure of the Quantum noise source and severe statistical weaknesses.

1.10.4 The samples drawn from the Quantum noise source during the start-up tests shall not be available for normal operations until the tests are completed; these samples may be discarded at any time, or may be used after the completion of the tests if there are no errors.

1.10.5 **Continuous health-tests** shall run indefinitely on the outputs of the Quantum noise source while the Quantum noise source is in operation. Continuous tests focus on the behaviour of the noise source and aim to detect failures as the noise source produces outputs. The purpose of continuous tests is to allow the Quantum entropy source to detect any kinds of failures in its underlying Quantum noise source.

1.10.6 The continuous health tests shall run continuously on all digitized samples obtained from the Quantum noise source, and so tests must have a very low probability of raising a false alarm during the normal operation of the noise source.

1.10.7 The continuous health tests shall atleast include the tests as specified in NIST SP 800-90B.

1.10.8 The optimal value for the false positive probability may depend on the rate that the Quantum entropy source produces its outputs. The false positive probability is recommended to be between 2^{-20} and 2^{-40}. Lower probability values are acceptable. The manufacturer shall specify a false positive probability suitable for their application.

1.10.9 The Quantum entropy source shall support **on-demand health tests**. The on-demand tests shall include at least the same testing done by the start-up tests. The entropy source may support on-demand testing by restarting the entropy source and rerunning the startup tests, or by rerunning the startup tests without restarting the entropy source. The manufacturer shall specify the approach used for on-demand testing.

1.10.10 The on-demand tests may include other tests defined by the developer, in addition to the testing done in the start-up tests.

1.10.11 Samples collected from the Quantum noise source during on-demand health tests shall not be available for use until the tests are completed; however these samples may be discarded at any time, or may be used after the completion of the tests providing that there are no errors.

1.10.12 If a failure of the Quantum entropy source occurs while the QRNG is being operated, the random bit stream shall be disabled immediately, until an appropriate set of health tests confirm resumption of normal operational state of QES.

1.10.13 Health tests shall be performed on the noise source samples before any post-processing is done. Additional health tests may be performed on the outputs of the post-processing function.

1.10.14 The Quantum entropy source's start-up tests shall run the continuous health tests over at least 1024 consecutive samples. The start-up tests may include other tests defined by the developer. The samples subjected to start-up testing may be released for operational use after the start-up tests have been passed, or may be discarded at any time.

1.10.15 When the health tests fail, the Quantum entropy source shall notify the consuming application of the error condition. The manufacturer may define different types of failures (e.g., intermittent and persistent), and the application is allowed to react differently to different types of failures (e.g., by inhibiting output for a short time). The health status may be included as a parameter in response to the request received from an application. Then application can decide whether to use the random numbers.

1.10.16 The manufacturer may define different cut-off values to detect intermittent and persistent failures. If so, these values (with corresponding false alarm probabilities) shall be specified in the submission documentation. If the Quantum entropy source detects intermittent failures and allows the Quantum noise source to return to normal functioning, the designer shall provide evidence that: a) The intermittent failures handled in this way are indeed extremely likely to be intermittent failures; and b) the tests will detect a permanent failure when one occurs, and will ultimately signal an error condition to the consuming application and cease operation. In the case where a persistent failure is detected, the Quantum entropy source shall not produce any outputs. The module may support being reset or returned to operation by the consuming application or system.

1.10.17 The manufacturer shall provide documentation that specifies all Quantum entropy source health tests and their rationale. The documentation shall include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at power-up continuously, or on-demand), and include rationale indicating why each test is believed to be appropriate for detecting one or more failures in the noise source.

1.10.18 The manufacturer shall provide documentation of any known or suspected noise source failure modes (e.g., the Quantum noise source starts producing periodic outputs like 101…01), and shall include developer-defined continuous tests to detect those failures. These should include potential failure modes that might be caused by an attack on the device.

1.10.19 Appropriate health tests that are tailored to the noise source should place special emphasis on the detection of misbehaviour near the boundary between the nominal operating environment and abnormal conditions. This requires a thorough understanding of the operation of the noise source.

1.11 Other Requirements

1.11.1 QRNG shall have an interface for entropy output and another interface for management purpose.

1.11.2 QRNG shall be compatible with the operating systems. The operating systems supported by the QRNG shall be specified by the manufacturer.

1.11.3 QRNG shall have a distributed architecture if it support multiple applications simultaneously.

1.11.4 QRNG may include an embedded NIST 800-90A approved DRBG along with a physical quantum entropy source, each with its own conceptual security boundary.

1.11.5 The construction of QRNG that includes DRBG mechanism shall be compliant to NIST SP 800-90C.

1.11.6 For an embedded DRBG, both the quantum entropy source and the DRBG shall contain their own health tests within their respective security boundaries as illustrated below:

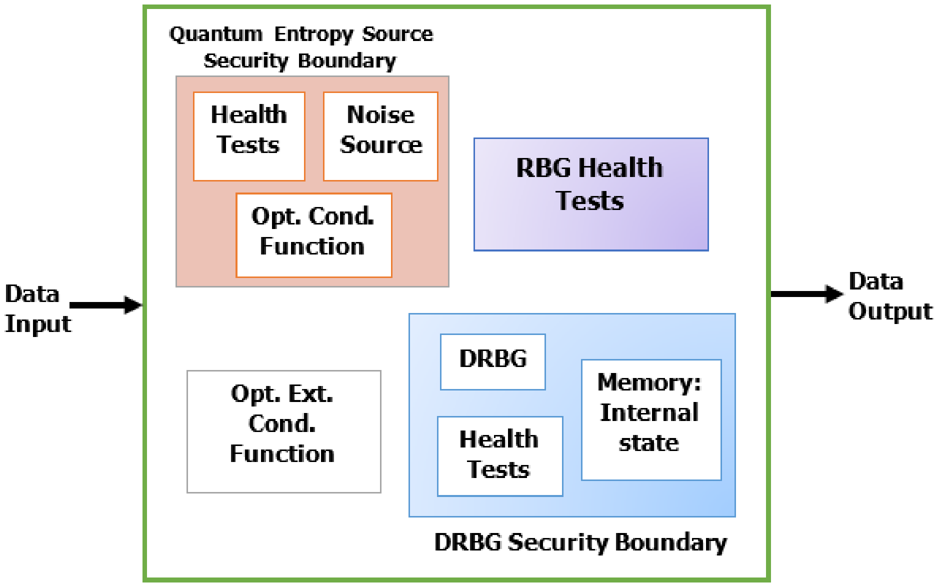

Figure 3: QRNG Security Boundary as per NIST SP 800-90C (4th Public Draft)

1.12 Statistical Testing of Randomness

1.12.1 The sequence at the output of QRNG must pass the following statistical test suites:

(i) NIST SP 800-22

(ii) Dieharder Tests

(iii) ENT Tests

(iv) Any other statistical tests, as prescribed.

1.12.2 The QRNGs adopting Quantum entanglement in the entropy generation process, shall include a CHSH Bell test. The test shall be defined for discrete variable (DV) or continuous variable (CV) according to the implementation..

1.13 Performance Requirements of QRNG

1.13.1 The validation of the Quantum entropy source may be carried out by the Manufacturer as per NIST SP 800-90B.

1.13.2 The QRNG shall deliver output with entropy per data bit very close to 1 with a high level of assurance. The average Shannon entropy and the average min-entropy per raw number bit after algorithmic post-processing (if any) shall exceed 0.9998, and 0.98 respectively.

NOTE: The algorithmic post-processing may be applied to the raw random numbers for the purpose of increasing the entropy per data bit (entropy extraction). The entropy measurement shall be made before any Cryptographic post-processing which is the stateful post-processing (i.e., with memory) for the purpose of gaining DRBG security properties (computational security).

1.13.3 The statistical properties of the raw random numbers shall not significantly change with the environmental conditions (e.g. temperature, voltage, etc.)

1.13.4 The total failure of the entropy source shall be immediately detectable. A degradation of the entropy source shall be detected sufficiently fast, where "sufficiently fast" depends on the degree of degradation.

1.13.5 The system shall raise alarm(s) in case of failures.

1.13.6 On detection of an error, the QRNG shall either (a) enter a permanent error state, or (b) be able to recover from a loss or compromise of entropy if the permanent error state is deemed unacceptable for the application requirements. These requirements may be satisfied procedurally or innately in the design.

1.13.7 The software/hardware in the equipment shall not pose any problem due to changes in date and time caused by events such as changeover of millennium/century, leap year etc. in the normal functioning of the equipment.

1.13.8 The QRNG shall have the provision to securely update the firmware.

1.13.9 Category-A QRNG shall support simultaneous multiple requests from applications.

1.13.10 An interface shall be available to obtain raw, digitized outputs from the quantum noise source. Such an interface shall be available only in "test mode" and it shall be disabled when the source is operational. The test mode may be disabled when QRNG is deployed in the field as per the requirement of the user.

1.13.11 If the QRNG is capable of operating in more than one mode, the QRNG should return information about the mode in which it is operating, upon request.

1.13.12 The QRNG shall supply random numbers through a secure standard interface and provide protection against unauthorised access including the identity authentication of the application.

1.13.13 The conditioned or the raw entropy may be delivered to applications/clients over a standard TCP/IP network connection with encryption protocols such as TLS or via mutually authenticated TLS.

1.13.14 The request for random numbers from the entropy output interface shall include the following parameters:

- — **size:** Number of random bits requested
- — **source:** the source of the random bits (processed or raw)
- — **format (optional):** binary, hex, JSON, etc.

1.13.15 The message in response to the request from the application shall include the following parameters:

- — unique ID of the Quantum Entropy Source
- — random bytes (encoded in base64 for JSON format)
- — mode (raw or processed random numbers)
- — timestamp
- — status (True if the request has been satisfied, otherwise false)
- — health status

1.13.16 An interface may optionally be available to request the entropy source to conduct a test of its health. The request for the health test may include:

Input: *type of test requested:* A bitstring that indicates the type or suite of tests to be performed

Output: *status:* A Boolean value that is TRUE if the entropy source passed the requested test, and is FALSE otherwise.

1.13.17 The system shall generate system logs for audit purpose. The logs may be classified with the appropriate labels eg. Request, Response, warning, Information, Error, Debug, etc.

1.13.18 The system shall support secured access along with user management and authentication.

1.13.19 The management shall be performed through a physical interface, web-based (HTTPS) interface, TLS-protected API calls, or via SSH command line.

1.13.20 Online Performance Monitoring: The QRNG system shall provide the facility for monitoring of system information and performance parameters. The performance parameters shall include the status of health tests, entropy output per bit, etc.

1.13.21 Suitable visual indications shall be provided, to indicate the healthy/ unhealthy conditions of the system.

1.14 Security Requirements of QRNG

1.14.1 The QRNG shall not leak relevant secret information (e.g., internal state) through the output.

1.14.2 The QRNG shall be resilient against side-channel and fault attacks.

1.14.3 The design and implementation of QRNG shall have a defined protection boundary. The protection boundary shall be as specified in ISO/IEC 19790.

1.14.4 The QRNG design shall include methods to prohibit predictable influence, manipulation, or predicting the output of the QRNG by observing the physical characteristics (e.g., power consumption, timing or emissions).

1.14.5 There shall be design evidence (theoretical, empirical, or both) to support all security requirements for the QRNG, including protection from misbehaviour.

1.14.6 Authentication mechanisms must be used to authenticate an operator accessing the system and to verify that the operator is authorized to access the system.

1.14.7 The QRNG shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the system (including substitution of the entire system) when installed. All hardware, software, firmware, and data components within the security boundary shall be protected. *[Category-A/B/C/D as applicable]*

1.14.8 The QRNG shall provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the system is attempted. *[Category-A & B]*

1.14.9 If the QRNG contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure. *[Category-A & B]*

1.15 Technical Specifications of QRNG

1.15.1 The manufacturer shall submit the following technical specifications of the QRNG offered for testing:

Details	Parameters		Specifications
Type of QRNG	Category A/B/C/D		
Entropy Source	Source of Quantum Randomness		
	Type of Quantum Entropy Source (QES1 or QES2) as per clause 1.6.6		
	Entropy Estimation of the Quantum Noise Source (as per clause 1.8.3)		
Performance	Average Shannon Entropy (as per clause 1.13.2)		
	Average Min-Entropy (as per clause 1.13.2)		
	Quantum Noise Source Bit Rate		
	Random post-processed bit rate	**Low rate**	< 10 Mbps
		Medium rate	10 – 100 Mbps
		High rate	100 – 1000 Mbps
		Very high rate	> 1 Gbps
	Number of simultaneous requests supported with key length		
	Latency - Time delay between request and response from QRNG (in µsec)		
Compliance	NIST SP800-90B Compliance		
	NIST SP 800-90 A/B/C Compliance		

	[in case of embedded DRBG]	
	NIST SP800-22 Statistical Test Suite Compliance	
	Die Harder Test suite Compliance	
	ENT Test suite Compliance	
Post-Processing	Post-Processing Algorithm used	
Type of Interface	Entropy Output	
	Management Interface	
	Other Interfaces	
Administration and Management	Command Line Interface (SSH)	
	Built –in web server	
	Syslog Alerting on GUI of remote monitoring system	
	Secured User Access Management	
Environmental	Operating temperature	
	Storage temperature	
	Humidity	
	Dimensions	
Physical Characteristics	Weight	
	Power Supply	
Power Consumption	Power consumption (Normal operation)	
	Power consumption (Idle Mode)	
	Details of OS supported along with versions	
OS supported		

CHAPTER-2

General Requirements

2.1 Reference documents

2.1.1 Whatever that has not been specifically stated in this document, shall be deemed to be as per relevant latest ITU-T Recommendations and NIST SP 800-90 A/B/C standard.

2.1.2 All references to TEC GRs & other Recommendations/standards imply their latest issues.

2.2 Engineering requirements

2.2.1 The manufacturer shall furnish the actual dimensions and weight of the equipment.

2.2.2 The equipment shall be 19'' rack mountable. *[Category A]*

2.2.3 The equipment shall have a robust chassis, redundant power supplies and hot-swap redundant fans. *[Category A]*

2.2.4 It should be engineered to comply with environmental test requirements as defined in this document.

2.2.5 The external plug-in units shall be of a suitable type to allow their removal/insertion while the equipment is in energized condition. *[Category A/B/C]*

2.2.6 The mechanical design and construction of each card/unit shall be inherently robust and rigid under all conditions of operation, adjustment, replacement, storage and transport.

2.2.7 Each sub-assembly shall be marked with schematic reference to show its function so that it is identifiable from the layout diagram in the handbook.

2.2.8 Each terminal block and individual tags shall be numbered suitably with a clear identification code and shall correspond to the associated wiring drawings. *[Category A/B/C]*

2.2.9 All external Interfaces / Controls / Indicators/Switches shall be clearly screen printed/marked on the unit to show their functional/connectivity diagrams and functions. *[Category A & B]*

2.2.10 Important Do's and Don'ts about the operation of the system shall be clearly indicated at a convenient place on the equipment. *[Category A & B]*

2.3 Operational requirements

2.3.1 The equipment shall be designed for continuous operation and shall be tested for 72 hours of continuous working.

2.3.2 The equipment shall be able to perform satisfactorily without any degradation at an altitude up to 4000 meters above mean sea level. A certificate from the manufacturer conforming to this requirement will be acceptable, in case no test facility is available.

2.3.3 Visual indication to show power ON/OFF status shall be provided.

2.3.4 QRNG shall be provided with software that includes drivers for the supported operating systems.

2.3.5 QRNG shall optionally provide a graphical interface to read and display random numbers and store them in a file.

2.3.6 Visual indications should be provided about the healthy and unhealthy conditions of the system.

2.4 Quality requirements

2.4.1 The manufacturer shall furnish the MTBF value along with the methodology used for calculation. The minimum value of MTBF shall be 25,000 hrs.

2.4.2 The equipment shall be manufactured in accordance with the international quality management system ISO 9001:2015 or latest issue. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted by the manufacturer.

2.5 Maintenance requirements

2.5.1 Maintenance philosophy is to replace faulty units/subsystems after quick online analysis through monitoring sockets, alarm indications and Built-in Test Equipment. *[Category A/B/C]*

2.5.2 The equipment shall have easy access for servicing and maintenance. *[Category A/B/C]*

2.5.3 The equipment shall have the provision to update the firmware.

2.5.4 Suitable alarms shall be provided for the identification of faults in the system and faulty units. The alarms may be placed on the QRNG Hardware and in the remote monitoring system.

2.5.5 Ratings and types of fuses used are to be indicated by the supplier.

2.6 Power supply requirements

2.6.1 The equipment should work at a single phase AC mains supply of 230 V with variation in the range of +15% and -15% and frequency as 50 Hz +/-2Hz or uninterrupted –48V DC with a variation in the range from -40V to -60V. *[Category A]*

2.6.2 The equipment shall operate over this range without any degradation in performance.

2.6.3 The equipment shall be adequately protected in case of voltage variation beyond the range mentioned above and also against input reverse polarity in case of DC feeds.

2.6.4 The derived DC voltages in the equipment shall have protection against over-voltage, short-circuit and overload.

2.6.5 The equipment shall be power efficient. The actual power rating/ consumption is to be furnished by the manufacturer of the equipment.

2.7 Accessories

2.7.1 The supplier shall provide a complete set of:

(a) all the necessary connectors, connecting cables (including power cord) and accessories required for satisfactory and convenient operation of the equipment. Types of connectors, adapters to be used and accessories of the approved quality shall be indicated in the operating manuals.

(b) Software, along with software version and the arrangement to load the software at site.

2.7.2 The source of the components/ accessories, from where these have been procured, is also to be submitted by the manufacturer.

2.8 Documentation

Technical literature in the English language only shall be accepted. All aspects shall be covered in the manuals. The manuals shall include the following :-

2.8.1 Installation, operation and maintenance manual

It should cover the following, as applicable to the category of the product:

(i) Safety measures to be observed in handling the equipment;

(ii) Precautions for installation, operation and maintenance;

(iii) Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance, troubleshooting and sub-assembly replacement;

(iv) Illustration of internal and external mechanical parts.

(v) The detailed description about the operation of the software used in the equipment including its configuration procedure, installation, loading and debugging, etc.

2.8.2 Repair Manual

It should cover the following, as applicable to the category of the product:

(i) List of replaceable parts used to include their sources and the approving authority.

(ii) Detailed ordering information for all the replaceable parts shall be listed in the manual to facilitate the reordering of spares.

(iii) Procedure for trouble-shooting and sub-assembly replacement shall be provided. Test fixtures and accessories required for repair shall also be indicated. A systematic troubleshooting chart (fault tree) shall be given for the probable faults with their remedial actions.

2.9 Operating personnel safety requirements

2.9.1 The Laser product, if used shall meet the Automatic Laser Shutdown (ALSD)/Automatic Power Reduction (APR) procedure of ITU-T Rec. G.664 (latest edition) on Class B laser. The equipment shall have visual warnings and controls ensuring danger-free operation. Laser safety signs and instructions must be mentioned in the equipment.

2.9.2 Protection against short circuits/open circuits in the access points shall be provided. *[Category A]*

2.9.3 The equipment shall have a terminal for grounding the rack. *[Category A]*

2.9.4 All switches/controls on the front panel shall have suitable safeguards against accidental operation. *[Category A]*

2.9.5 The equipment shall be adequately covered to safeguard against entry of dust, insects, etc. *[Category A/B]*

2.10 Environmental Testing Requirements

2.10.1 The instrument shall conform to the requirements for the applicable category as specified in TEC document TEC 14016:2010 {Old Document No: QM-333) {MARCH 2010 issue} "Standard for Environmental Testing of Telecommunication Equipment".

CHAPTER-3

Safety & EMC Requirements

3.1 Safety Requirements *[Category A/B/C]*

3.1.1 The equipment shall conform to IS/IEC 62368-1:2023 "Audio/video, information and communication technology equipment - Part 1: Safety requirements".

3.1.2 Laser safety: If the QRNG house active optical devices with optical signal coming out of the enclosure, it should comply with IEC 60825- 1 and IS 14624-2/IEC 60825-2 for optical safety requirements.

Note: This test shall be applicable if Laser components are directly mounted in the box.

3.2 Electromagnetic Compatibility (EMC) Requirements: *[Category A & B]*

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from an accredited test agency.

3.2.1 **Conducted and radiated emission (applicable to telecom equipment):**

Name of EMC Standard: "CISPR 32:2015+A1:2019 - Electromagnetic compatibility of multimedia equipment - Emission requirements"

i. To comply with Class B of CISPR 32:2015+A1:2019.

ii. For Radiated Emission tests, limits below 1 GHz shall be for measuring a distance of 3m.

OR

Conducted and Radiated Emission (applicable to instruments such as power meter, frequency counter, etc.):

Name of EMC Standard: " CISPR 11 {2024} - Industrial, scientific and medical (ISM) radio-frequency equipment - Electromagnetic disturbance characteristics- Limits and methods of measurement"

Limits:

i. To comply with the category of Group 1 of Class B of CISPR 11 {2024}

ii. The values of limits shall be as per clause No. 8.5.2 of TEC Standard No. TEC 11016:2026.

3.2.2 Immunity to Electrostatic discharge:

Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test"

Limits:

i. Contact discharge level 2 {± 4 kV} or higher voltage;

ii. Air discharge level 3 {± 8 kV} or higher voltage;

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.

3.2.3 **Immunity to radiated RF:**

Name of EMC Standard: IEC 61000-4-3 (2020) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits:

(i) For Telecom Equipment and Telecom Terminal Equipment with Voice interface(s)

a. Under test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and

b. Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in the frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

(ii) For Telecom Terminal Equipment without Voice interface (s)

a. Under test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and protection against digital radio telephones and other RF devices in the frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.

3.2.4 **Immunity to fast transients (burst):**

Name of EMC Standard: IEC 61000- 4- 4 (2012) "Testing and measurement techniques of electrical fast transients / burst immunity test"

Limits:

i. Test Level 2 i.e., a) 1 kV for AC/DC power lines; b) 0.5 kV for signal / control / data / telecom lines.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.

3.2.5 **Immunity to surges:**

Name of EMC Standard: IEC 61000-4-5 (2014) "Testing & Measurement techniques for Surge immunity test"

Limits:

(i) For mains power input ports:

(a) 1.0 kV peak open circuit voltage for a line-to-ground coupling.

(b) 0.5 kV peak open circuit voltage for a line-to-line coupling.

(c) 2.0 kV peak open circuit voltage for a line-to-line coupling.

(ii) For telecom ports:

(a) 1.0 kV peak open circuit voltage for line to ground.

(b) 0.5 kV peak open circuit voltage for line-to-line coupling.

(c) 2.0 kV peak open circuit voltage for line-to-line coupling.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2026.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2026.

3.2.6 Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2023) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio-frequency fields"

Limits:

i. Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2026.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2026.

3.2.7 **Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):**

Name of EMC Standard: IEC 61000-4-11 (2020) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests"

Limits:

i. A voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70 % supply voltage for 500ms)
ii. A voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e., 40% supply voltage for 200ms)
iii. A voltage interruption corresponding to a reduction of a supply voltage of > 95% for 5s.
iv. A voltage interruption corresponding to a reduction of a supply voltage of >95% for 10ms.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2026.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2026.

3.2.8 **Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):**

Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on DC input power port immunity tests

Limits:

i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.

ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C.

iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B.

iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000 ms. Applicable Performance Criteria shall be C.

v. Voltage variations correspond to 80% and 120% of supply for 100 ms to 10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B.

Note 1: Classification of the equipment:

Class B: Class B is a category of apparatus which satisfies the class B disturbance limits. Class B is intended primarily for use in the domestic environment and may include:

i. Equipment with no fixed place of use; for example, portable equipment powered by built in batteries;

ii. Telecommunication terminal equipment is powered by telecommunication networks.

iii. Personal computers and auxiliary connected equipment.

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Class A: Class A is a category of all other equipment, which satisfies the class A limits but not the class B limits.

Note 2: The testing agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted.

Note 3: For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. 11016:2016 (or latest release) and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per the above mentioned sub clauses 3.2.1 to 3.2.9 and TEC Standard No. 11016:2016 (or latest release). The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 22	EN 55022
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11
IEC 61000-4-29	EN 61000-4-29

DEFINITIONS, ACRONYMS AND TERMINOLOGY

DEFINITIONS

Adversary: A malicious entity whose goal is to determine, to guess, or to influence the output of an RNG.

Algorithm: A clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result.

Authentication: The corroboration that a peer entity in an association is the one claimed (peer-entity authentication). The corroboration that the source of data received is as claimed (data origin authentication).

Assessment (of entropy): An evaluation of the amount of entropy provided by a (digitized) noise source and/or the entropy source that employs it.

Backward secrecy: assurance that previous values cannot be determined from knowledge of the current value or subsequent values.

Binary data (from a noise source): Digitized output from a noise source that consists of a single bit; that is, each sampled output value is represented as either 0 or 1.

Bitstring: An ordered and finite sequence of 0's and 1's. The leftmost bit is the most significant bit.

Block cipher: A parameterized family of permutations on bitstrings of a fixed length; the parameter that determines the permutation is a bitstring called the key.

Conditioning (of noise source output): A method of processing the raw data to reduce bias and/or ensure that the entropy rate of the conditioned output is no less than some specified amount.

Consuming Application: An application that uses random outputs from an RNG.

Continuous Test: A type of health test performed within an entropy source on the output of its noise source in order to gain some level of assurance that the noise source is working correctly, prior to producing each output from the entropy source.

Cryptographic: State transition functions and output functions are considered cryptographic if they are composed of cryptographic primitives (e.g. block ciphers or hash functions).

Cryptographic post-processing: Stateful post-processing (i.e., with memory) for the purpose of gaining DRNG security properties (computational security). It is usually applied to intermediate random numbers, or to internal random numbers of a separate TRNG. It can also be applied to raw random numbers.

Deterministic RNG: An RNG that produces random numbers by applying a deterministic algorithm from a secret initial value called a seed, along with other possible additional input.

Digitization: The process of generating raw discrete digital values from non-deterministic events (e.g. analog noise sources) within a noise source.

DRBG mechanism: The portion of an RNG that includes the functions necessary to instantiate and uninstantiate the RNG, generate pseudorandom bits, (optionally) reseed the RNG and test the health of the DRBG mechanism.

Entropy: A measure of the disorder, randomness or variability in a closed system. Min-entropy is the measure used in this document.

Entropy rate: The rate at which a digitized noise source (or entropy source) provides entropy; it is computed as the assessed amount of entropy provided by a bitstring output from the source, divided by the total number of bits in the bitstring (yielding the assessed bits of entropy per output bit). This will be a value between zero (no entropy) and one.

Entropy source: The combination of a noise source, health tests, and an optional conditioning component that produces random bit strings to be used by a random bit generator.

Estimate: The estimated value of a parameter, as computed using an estimator.

Estimator: A technique for estimating the value of a parameter.

False Positive: An erroneous acceptance of the hypothesis that a statistically significant event has been observed. This is also referred to as a type 1 error. When "health-testing" the components of a device, it often refers to a declaration that a component has malfunctioned – based on some statistical test(s) – despite the fact that the component was actually working correctly.

Forward secrecy: assurance that the knowledge of subsequent (future) values cannot be determined from current or previous values.

Hash Function: A (mathematical) function that maps values from a large (possibly very large) domain into a smaller range.

Health testing: Testing within an implementation immediately prior to or during normal operation to determine that the implementation continues to perform as implemented and as validated.

Initial value (Initialisation value): Value used in defining the starting point of a cryptographic algorithm (e.g., a hash-function or an encryption algorithm).

Intermediate Random Number: Input data for cryptographic post-processing

Internal Random Number: Final stage of the random numbers of an RNG that are ready to be output. The sequence of internal random numbers depends only on the noise source, seeding procedure, reseeding procedure, or additional input. Compare to external random numbers.

Internal state: The collection of all secret and non-secret digitized information of an RNG as stored in memory at a given point in time.

Instantiate: The process of initializing a DRBG with sufficient randomness to generate pseudorandom bits at the desired security strength.

Min-entropy: The min-entropy of a random variable is a lower bound on its entropy. The precise formulation for min-entropy is ($\log_2$ max p_i) for a discrete distribution having probabilities p_1, …,p_k. Min-entropy is often used as a worst-case measure of the unpredictability of a random variable.

Narrowest internal width: The maximum amount of information from the input that can affect the output.

Noise Source: A source of unpredictable data that outputs raw discrete digital values. The digitization mechanism is considered part of the noise source. A distinction is made between physical noise sources and non-physical noise sources.

Non-physical noise source: A noise source that typically exploits system data and/or user interaction to produce digitized random data.

On-demand test: A type of health test that is available to be run whenever a user or a relying component requests it.

Output space: The set of all possible distinct bitstrings that may be obtained as samples from a digitized noise source.

Physical entropy sources: An entropy source that uses dedicated hardware or uses a physical experiment (noisy diode(s), oscillators, event sampling like radioactive decay, etc.).

Physical Noise Source: A noise source that exploits physical phenomena (thermal noise, shot noise, jitter, metastability, radioactive decay etc.) from dedicated hardware designs (using diodes, ring oscillators etc.) or physical experiments to produce digitized random data.

Post-processing: Generic term for any kind of transformation applied to random numbers of different stages in the generation of internal random numbers in a TRNG (e.g., to raw random numbers).

Probability distribution: A function that assigns a probability to each measurable subset of the possible outcomes of a random variable.

Pseudorandom: A deterministic process (or data produced by such a process) whose output values are effectively indistinguishable from those of a random process as long as the internal states and internal actions of the process are unknown. For cryptographic purposes, “effectively indistinguishable” means “not within the computational limits established by the intended security strength.”

Quantum entropy source (QES): An entropy source based on at least one quantum phenomenon. Examples of quantum phenomena include quantum state superposition, quantum state entanglement, Heisenberg uncertainty, quantum tunnelling, spontaneous emission or radioactive decay.₩

QES1: A subclass of quantum entropy sources that will assess a given minimum entropy amount by measuring the implementation imperfections and verifying that they are within defined acceptable value ranges.

QES2: A subclass of quantum entropy sources that will assess their generated entropy amount by measuring signatures of the quantum process.

Randomness: It is the unpredictability of a bitstring. If the randomness is produced by a non-deterministic source (e.g., an entropy source), the unpredictability is dependent on the quality of the source.

Random Number Generator (RNG): A device or algorithm that outputs a random sequence that is effectively indistinguishable from statistically independent and unbiased bits.

Raw data: Digitized output of the noise source.

Raw Random Number: Raw random numbers are discrete values (usually bits, bit strings, or integers) which are derived at discrete points in time from a noise source of a QRNG. Raw random numbers have not been significantly post-processed.

Reseed: To refresh the internal state of a DRBG with seed material. The seed material should contain sufficient entropy to allow recovery from a possible compromise.

Sample: An observation of the raw data output by a noise source. Common examples of output values obtained by sampling are single bits, single bytes, etc. (The term "sample" is often extended to denote a sequence of such observations; this Recommendation will refrain from that practice.)

Security Boundary: A physical or conceptual perimeter that confines the secure domain which an adversary cannot observe or influence in a malicious way (according to the chosen threat model). Or

A conceptual boundary that is used to assess the amount of entropy provided by the values output from an entropy source. The entropy assessment is performed under the assumption that any observer (including any adversary) is outside of that boundary

Seed: Initializing the internal state of a DRNG with seed material. The seed material should contain sufficient entropy to meet security requirements.

Security strength: A number associated with the amount of work (i.e., the number of basic operations of some sort) that is required to "break" a cryptographic algorithm or system in some way.

Seed material: A bitstring that is used as input to a DRBG. The seed material determines a portion of the internal state of the DRBG.

Shannon Entropy: A measure of entropy based on the expected (average) gain of information from an observation.

Signature of a quantum process: A set of measurable statistical properties that are characteristic of a given quantum process according to some assumptions provided in the description, and that permits quantification of this process' impact on the measurement outputs in a manner that enables a direct or indirect estimation of the minimum amount of entropy coming solely from the quantum process. For example, one signature of quantum entanglement is the violation of Bell inequalities.

Start-up testing: A suite of health tests that are performed every time the entropy source is initialized or powered up. These tests are carried out on the noise source before any output is released from the entropy source.

Stochastic Model: A stochastic model provides a partial mathematical description (of the relevant properties) of a (physical) noise source using random variables. It allows the verification of a (lower) entropy bound for the output data (internal random numbers or intermediate random numbers). Formally, a stochastic model consists of a family of probability distributions that contains the true distribution of the noise source output (raw random numbers) or of suitably defined auxiliary random variables during the lifetime of the physical RNG, even if the quality of the digitized data goes down. The stochastic model is based on and justified by the understanding of the noise source.

Total Failure: The noise source is broken and delivers no or at most a small fraction of its previous entropy

True RNG: A device or mechanism for which the output values depend on a noise source.

Unbiased: A random variable is said to be unbiased if all values of the finite sample space are chosen with the same probability. Contrast with biased.

Uninstantiate: The termination of a DRBG instantiation.

With memory: Property of a post-processing algorithm. It means that the post-processing is stateful, i.e. has a state that retains information from previous invocations or steps.

ABBREVIATIONS

For the purpose of this document the following abbreviations apply:

AC	Alternating Current
ALSD	Accessible Light Source Distance
APR	Average Power Ratio
BSNL	Bharat Sanchar Nigam Limited
CISPR	International Special Committee on Radio Interference
DRBG	Deterministic Random Bit Generator
DC	Direct Current
EMC	Electromagnetic Compatibility
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
GR	Generic Requirement
Hz	Hertz
IEC	International Electrotechnical Commission
IID	Independent and Identically Distributed
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
PRNG	Pseudo Random Number Generator
QES	Quantum Entropy Source
QES1	Type 1 Quantum Entropy Source
QES2	Type 2 Quantum Entropy Source

QRNG	Quantum Random Number Generator
RNG	Random Number Generator
SSH	Secure Shell
TRNG	True Random Number Generator
USB	Universal Serial Bus

----End of the document----