K. J. Somaiya College of Engineering, Mumbai-77
(A constituent college of Somaiya Vidyavihar University)

Batch: B1	**Roll No.: 16010121045**
Experiment No: 02	
Group No:	

Title: Design Document for MiniProject.

Objective: Understand the necessity of design document.

Expected Outcome of Experiment:

Books/ Journals/ Websites referred:

1.
2.
3.

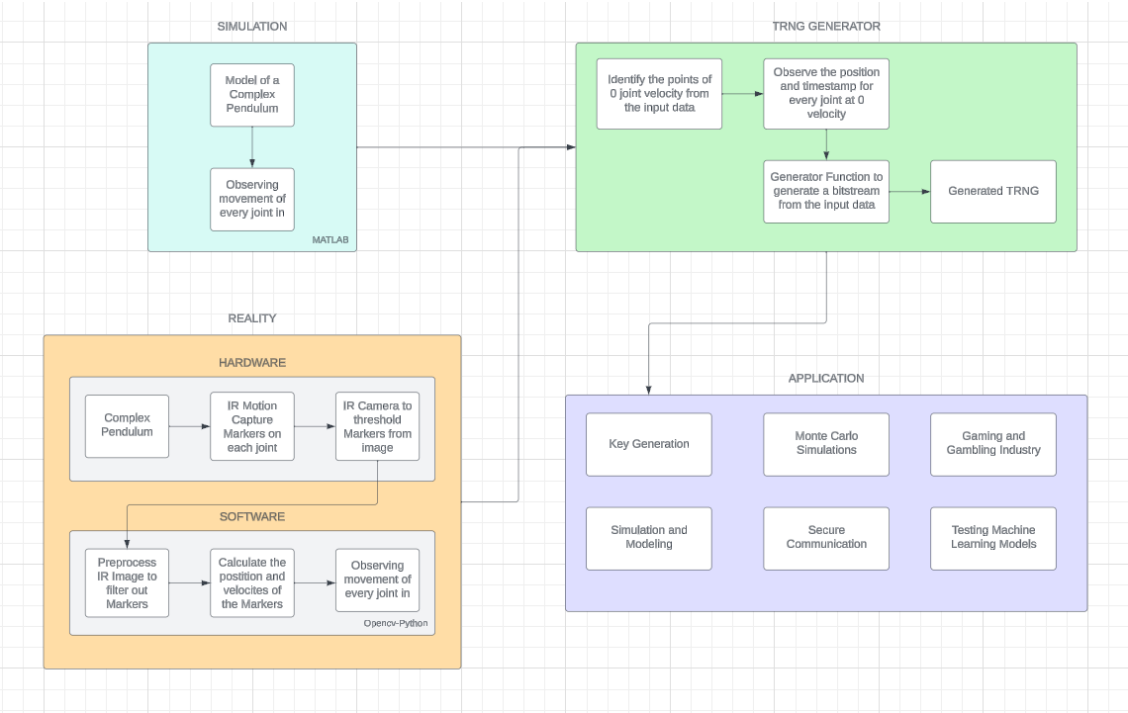
Introduction:

As the process of development of a project progresses, the second important stage is the design.

In this document, Following designs are expected to be prepared:

1. Frontend interface
2. Backend/ database design /Data design
3. Architectural design.
4. UML diagrams
5. Design of test cases.
6. Algorithmic design
   (As per the requirement of the application)

Snapshots of design:



Test Cases :

Designing test cases for a True Random Number Generator (TRNG) application involves verifying its ability to generate truly random numbers with desired properties such as unpredictability, uniform distribution, and independence. Here's a set of test cases covering various aspects of TRNG functionality:

1. **Basic Functionality**
   - Test Case 1: Verify that the TRNG application produces a sequence of numbers.
   - Test Case 2: Confirm that the generated numbers are within the expected range (e.g., 0 to 255 for byte-sized outputs).
   - Test Case 3: Ensure that the output sequence contains a sufficient number of values for the intended application.
2. **Statistical Properties**
   - Test Case 4: Perform a frequency test to verify that each possible output value occurs with approximately equal probability.
   - Test Case 5: Conduct a runs test to check for patterns or sequences in the generated numbers.
   - Test Case 6: Use an autocorrelation test to ensure that successive numbers in the sequence are statistically independent.
3. **Uniformity and Distribution**

- Test Case 7: Test for uniformity by partitioning the output range into intervals and counting the number of generated values falling into each interval.
- Test Case 8: Evaluate the distribution of generated numbers using statistical tests such as chi-square or Kolmogorov-Smirnov tests.

4. **Entropy and Randomness**
   - Test Case 9: Measure the entropy of the generated sequence to assess its randomness and information content.
   - Test Case 10: Validate the unpredictability of the TRNG output by comparing consecutive sequences generated under similar conditions.
5. **Robustness and Stability**
   - Test Case 11: Stress test the TRNG application by running it for an extended period to check for any degradation or bias in the generated sequence over time.
   - Test Case 12: Evaluate the TRNG's performance under various environmental conditions (e.g., temperature variations, electromagnetic interference) to ensure robustness.
6. **Integration and Compatibility**
   - Test Case 13: Verify that the TRNG application integrates smoothly with other systems or applications that consume its output.
   - Test Case 14: Test compatibility with different platforms, operating systems, or hardware configurations.
7. **Security and Cryptographic Properties**
   Test Case 15: Assess the TRNG's suitability for cryptographic applications by subjecting its output to cryptographic analysis and randomness tests specified in cryptographic standards (e.g., NIST SP 800-22).
8. **Error Handling and Recovery**
   - Test Case 16: Validate the TRNG's error handling mechanisms by injecting faults or disturbances and observing its behavior and recovery strategies.

Conclusion:

In conclusion, the project will aim to explore the utilization of a complex pendulum integrated with infrared (IR) marker-based motion capture technology to generate True Random Number Generators (TRNGs). By leveraging the chaotic behavior of the pendulum and capturing precise data on joint positions and velocities using IR markers, the project intends to produce random numbers rooted in physical dynamics rather than algorithmic processes alone.

Throughout the project, several key objectives are expected to be achieved. The implementation of the complex pendulum will provide a natural source of unpredictability, as its motion will be influenced by a multitude of factors such as initial

conditions and environmental variables. This inherent randomness will be further augmented by the accurate measurement of joint positions and velocities via IR markers, ensuring that the generated random numbers are based on real-world dynamics.

By selecting timestamps corresponding to instances when joint velocities reach zero, the project plans to identify significant events in the pendulum's motion as reference points for extracting random data. These moments of stability or equilibrium will serve as robust foundations for the random number generation process, enhancing the integrity and authenticity of the output.

The project's approach is expected to offer several notable advantages. It will provide a unique blend of physical dynamics and computational processes, resulting in random number generation that is scientifically grounded and practically applicable across various domains. Moreover, the utilization of motion capture technology will ensure high-resolution data capture, leading to accurate and reliable results.

In conclusion, the project aims to demonstrate the feasibility and effectiveness of using a complex pendulum with IR marker-based motion capture technology for TRNG generation. While further refinements and optimizations may be warranted, the project will lay a solid foundation for future research and applications in the field of random number generation, offering a promising avenue for exploring the intersection of physical systems and computational methods in generating truly random numbers.