Renesas RA Family

NIST SP800-22r1a Random Number Statistical Test Report for RA4E2

Target product		RA4E2
Evaluation sample	**Brief**	The random sequence gained from RA4E2.
	Original file	RA4E2_Random_Number_Data_20230622.1Gbit.zip
	Binary file	RA4E2_Random_Number_Data_20230622.1Gbit.bin
	Provided by	REE/IIBU/IOTBD/IPM1/IPM12
	Date gained	June 22, 2023
Evaluation department		Renesas Electronics Corporation Embedded Processing, Digital Power and Signal Chain Solutions Group Shared R&D Core Technology Division Security Competence Center
Test started on		July 23, 2023
Test completed on		July 23, 2023
Result		PASS From the result obtained by the test tool shown below, the tester confirmed that the result was PASS.

The following standard and tool were used for this statistical test of the evaluation sample:

- Special Publication 800-22 Revision 1a
  A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Revised: April 2010, NIST
- Test tool: sts-2.1.2
  The tool is downloadable from the following web site:
  https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software

1. Introduction

1.1 Test Description

This is the report of the SP 800-22 based statistical tests for the evaluation sample.

Note: The evaluation sample is the random sequence generated by the RNG implemented in the target product for SP800-22 test suite. The file was converted to a binary format by the evaluation department.

The test was conducted by REL/EPSG/SRCTE/SSCC, based on NIST SP 800-22 Revision 1a [SP800-22]: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, revised: April 2010, published by NIST.

The test was conducted by utilizing the test tool downloaded from the following NIST web page [STS2.1.2]: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.

The following 15 statistical tests are described in Chapter 2 of [SP 800-22].

Table 1. Statistical Tests of [SP800-22]

No	Statistical Tests
1	Frequency (Monobit) Test
2	Frequency Test within a Block
3	Runs Test
4	Test for the Longest Run of Ones in a Block
5	Binary Matrix Rank Test
6	Discrete Fourier Transform (Spectral) Test
7	Non-overlapping Template Matching Test
8	Overlapping Template Matching Test
9	Maurer's "Universal Statistical" Test
10	Linear Complexity Test
11	Serial Test
12	Approximate Entropy Test
13	Cumulative Sums (Cusum) Test
14	Random Excursions Test
15	Random Excursions Variant Test

1.2 Test Method

The test tool tests and determines the randomness by utilizing the proportion of sequences that pass a statistical test and the distribution of P-value to check the uniformity, as described in Section 4.2 of [SP800-22]. (Refer to [SP800-22] for details).

1.3 Test Strategy

The test tool can perform all statistical tests in a single execution. In this case, the common parameters of all statistical tests are sequence length and sample size. These parameters are mandatory to be used.

The tester selected 1,000,000 bits as the sequence length. This value of the sequence length is the maximum recommended length of each statistical test in [SP800-22].

The tester selected 1,000 as the sample size. Since the significance level is 0.001, the sample size 1,000 is the minimum size that is statistically meaningful. This significance level of 0.001 is default value.

The tester selected default values not only for the significance level but also for the other parameters in each statistical test.

2. Test results from the test tool

2.1 Test preparation

The evaluation sample sent from client department was a hexadecimal text file. So, the evaluation department converted it to a binary file and stored in the web storage of the testing department. The tester applied this binary file to the test tool.

2.2 Test results

The parameters were selected according to the test strategy described in section 1.3. That is, the sequence length was 1,000,000 bits, the sample size was 1,000, and the other parameters were default values. As shown in the test method described in section 1.2, the test result is judged by the proportion of the sequences and the distribution of P-value.

According to the test tool, the PASS reference values are as follows:

Note: The PASS values of the proportion of the sequences were calculated and output to the report file (finalAnalysisReport.txt) by the test tool. The PASS values of the proportion of the sequences shown in Table 2 are values from this output file.

Table 2. PASS Reference Values

Decided value	PASS value	Note
Distribution of P-value	≥ 0.0001	
Proportion of the sequences	≥ 980	Each statistical test except for the random excursion (variant) test.
	≥ Differ by each trial. For the value, refer to Appendix A.1.	Random excursion (variant) test.

The details of the proportion of the sequences and the distribution of P-value calculated by the Test Tool are shown in Appendix A.

According to the reference values shown in Table 2, all test results satisfied the reference value.

3. Conclusions

All test results satisfied the reference value. Therefore, the result was PASS.

Appendix A

When the test is completed, the test tool outputs the test summary (finalAnalysisReport.txt). Below is the test summary for the evaluation sample.

Appendix A.1 Sequence length = 1,000,000 / Sample size = 1,000

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <RA4E2_Random_Number_Data_20230622.1Gbit.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 91  92  93 109 108 111 107 101 104  84  0.552383    994/1000    Frequency
105  97  95  91  88 115  99 105 111  94  0.645448    987/1000    BlockFrequency
 93  85 108 101 104 118 107  98  97  89  0.473064    993/1000    CumulativeSums
 99  88 112 104  96  90 107 111  91 102  0.662091    992/1000    CumulativeSums
 98 105 105  94  97 101 103  94 117  86  0.709558    991/1000    Runs
106 108 101 100  95 104 107  84 103  92  0.816537    991/1000    LongestRun
102  92 100 100 114  83  92 107 104 106  0.618385    985/1000    Rank
116 111  87  93 120  97 107  79  90 100  0.068145    986/1000    FFT
116  98  97  94  89 106  91 104 103 102  0.767582    990/1000    NonOverlappingTemplate
101  95 102 104 104  93 101 106  93 101  0.991780    991/1000    NonOverlappingTemplate
112  85  84 114  93 104  98  99 102 109  0.370262    992/1000    NonOverlappingTemplate
108  98 105  96 106 104  94  94  97  98  0.981940    990/1000    NonOverlappingTemplate
103 102 105 101 100  97 103  97  87 105  0.978072    993/1000    NonOverlappingTemplate
 94  87  88  98 104 103  97 112 104 113  0.620465    991/1000    NonOverlappingTemplate
115  93  83 117 114 101 110  83  89  95  0.070299    989/1000    NonOverlappingTemplate
103  87 110  77 101 105 107  92 110 108  0.268917    990/1000    NonOverlappingTemplate
123  88  99  90 102  93 103  98  94 110  0.370262    987/1000    NonOverlappingTemplate
 88 115  96 114  97 103  79  93 113 102  0.180568    990/1000    NonOverlappingTemplate
112 103  89  84 106  84 118  91 107 106  0.157251    988/1000    NonOverlappingTemplate
101  89 100 102 103  90 115  95  86 119  0.317565    994/1000    NonOverlappingTemplate
100  89  90  89  98  90 106  96 113 129  0.088762    990/1000    NonOverlappingTemplate
 94  87 101 107 115  89 113  99  93 102  0.510153    989/1000    NonOverlappingTemplate
 95  77  79 103 106 114 100  85 125 116  0.005319    991/1000    NonOverlappingTemplate
110 108  95 108 114  98  88 102  92  85  0.446556    988/1000    NonOverlappingTemplate
104 102 106 103  93  98 102  90 104  98  0.982958    988/1000    NonOverlappingTemplate
108  93  86  94  99 103  88 101 111 117  0.428095    990/1000    NonOverlappingTemplate
 98  90 129  99  96 106  90  93 110  89  0.134172    989/1000    NonOverlappingTemplate
112 111  94  97 108  85 101 105  83 104  0.410055    987/1000    NonOverlappingTemplate
109  98 102  84 101  97 109  88 105 107  0.684890    985/1000    NonOverlappingTemplate
```

99	99	105	112	95	92	95	87	113	103	0.707513	991/1000	NonOverlappingTemplate
112	90	104	81	93	121	99	106	105	89	0.165340	993/1000	NonOverlappingTemplate
96	96	85	102	110	93	95	114	110	99	0.603841	989/1000	NonOverlappingTemplate
96	104	89	103	107	117	102	103	81	98	0.457825	990/1000	NonOverlappingTemplate
100	94	109	90	109	95	95	101	97	110	0.869278	994/1000	NonOverlappingTemplate
104	95	103	105	95	109	86	95	95	113	0.743915	989/1000	NonOverlappingTemplate
90	105	95	114	105	82	100	97	100	112	0.486588	991/1000	NonOverlappingTemplate
94	94	96	105	94	108	96	95	121	97	0.632955	991/1000	NonOverlappingTemplate
94	91	105	97	116	100	90	105	104	98	0.786830	992/1000	NonOverlappingTemplate
94	84	103	109	103	100	121	88	101	97	0.361938	987/1000	NonOverlappingTemplate
114	100	109	91	104	91	95	106	108	82	0.433590	983/1000	NonOverlappingTemplate
106	86	106	90	83	104	102	114	108	101	0.402962	982/1000	NonOverlappingTemplate
122	79	106	101	90	107	106	96	104	89	0.162606	985/1000	NonOverlappingTemplate
95	98	113	92	97	95	96	107	97	110	0.859637	990/1000	NonOverlappingTemplate
100	98	100	99	91	106	117	89	98	102	0.798139	989/1000	NonOverlappingTemplate
94	93	102	109	100	104	89	96	97	116	0.751866	993/1000	NonOverlappingTemplate
97	105	89	100	111	104	97	108	87	102	0.800005	989/1000	NonOverlappingTemplate
82	101	138	93	96	98	97	97	92	106	0.020831	992/1000	NonOverlappingTemplate
96	103	91	102	86	89	121	113	105	94	0.277082	992/1000	NonOverlappingTemplate
96	92	111	101	97	89	93	106	100	115	0.697257	986/1000	NonOverlappingTemplate
103	86	96	113	97	106	107	94	95	103	0.784927	987/1000	NonOverlappingTemplate
114	97	87	112	95	89	117	93	87	109	0.185555	988/1000	NonOverlappingTemplate
99	97	115	96	83	108	106	105	98	93	0.618385	989/1000	NonOverlappingTemplate
103	117	100	92	89	95	98	106	94	106	0.719747	991/1000	NonOverlappingTemplate
113	102	89	102	110	94	107	104	94	85	0.574903	987/1000	NonOverlappingTemplate
94	110	96	100	101	95	108	101	108	87	0.854708	988/1000	NonOverlappingTemplate
91	106	95	101	104	97	92	98	122	94	0.579021	994/1000	NonOverlappingTemplate
106	98	92	82	95	90	112	123	100	102	0.196920	982/1000	NonOverlappingTemplate
82	99	114	89	109	104	105	100	99	99	0.568739	992/1000	NonOverlappingTemplate
92	91	97	106	100	103	99	113	98	101	0.927677	993/1000	NonOverlappingTemplate
95	97	117	110	92	104	104	90	105	86	0.494392	993/1000	NonOverlappingTemplate
102	86	95	105	101	93	97	106	107	108	0.869278	990/1000	NonOverlappingTemplate
82	115	100	88	97	133	109	77	97	102	0.004085	992/1000	NonOverlappingTemplate
110	90	105	100	102	101	97	102	106	87	0.877083	991/1000	NonOverlappingTemplate
98	97	98	104	105	100	112	112	85	89	0.645448	982/1000	NonOverlappingTemplate
105	101	102	98	107	95	85	98	101	108	0.910091	990/1000	NonOverlappingTemplate
98	123	92	99	95	105	95	97	101	95	0.628790	986/1000	NonOverlappingTemplate
101	106	112	103	97	97	86	90	101	107	0.784927	993/1000	NonOverlappingTemplate
91	97	98	98	93	113	104	103	96	107	0.907419	991/1000	NonOverlappingTemplate
100	99	107	101	97	98	92	96	94	116	0.886162	992/1000	NonOverlappingTemplate
87	113	92	107	114	94	100	85	104	104	0.401199	993/1000	NonOverlappingTemplate
88	103	85	106	110	108	103	96	98	103	0.723804	988/1000	NonOverlappingTemplate
90	94	94	98	108	105	99	93	117	102	0.731886	993/1000	NonOverlappingTemplate
96	120	98	108	77	95	101	85	118	102	0.068571	987/1000	NonOverlappingTemplate
101	100	106	99	102	97	97	94	106	98	0.998058	990/1000	NonOverlappingTemplate
105	83	106	100	83	117	96	96	113	101	0.255705	990/1000	NonOverlappingTemplate
107	85	92	109	103	108	96	95	103	102	0.792508	985/1000	NonOverlappingTemplate
114	91	85	105	88	106	113	79	118	101	0.058612	991/1000	NonOverlappingTemplate
95	105	118	113	95	100	82	80	105	107	0.134944	996/1000	NonOverlappingTemplate
110	87	89	96	96	100	115	106	96	105	0.612147	996/1000	NonOverlappingTemplate
111	109	103	100	94	108	75	91	114	95	0.192724	991/1000	NonOverlappingTemplate
104	90	92	87	109	107	100	93	103	115	0.572847	989/1000	NonOverlappingTemplate
105	98	121	107	74	96	104	92	115	88	0.055361	987/1000	NonOverlappingTemplate
116	97	98	94	89	106	90	105	103	102	0.739918	990/1000	NonOverlappingTemplate
107	96	89	111	94	98	101	95	113	96	0.781106	986/1000	NonOverlappingTemplate
101	114	82	102	108	78	117	112	90	96	0.062427	992/1000	NonOverlappingTemplate
103	85	106	90	116	116	95	107	96	86	0.231956	992/1000	NonOverlappingTemplate
111	97	88	103	94	105	108	102	102	90	0.820143	992/1000	NonOverlappingTemplate

96	99	98	101	97	95	113	87	111	103	0.812905	991/1000	NonOverlappingTemplate
118	108	74	105	90	86	99	103	108	109	0.080519	989/1000	NonOverlappingTemplate
95	115	100	98	91	112	104	97	100	88	0.691081	989/1000	NonOverlappingTemplate
107	110	98	116	91	109	77	96	90	106	0.185555	989/1000	NonOverlappingTemplate
79	97	101	92	103	109	102	100	110	107	0.576961	991/1000	NonOverlappingTemplate
97	113	90	98	114	114	97	108	77	92	0.145326	991/1000	NonOverlappingTemplate
101	99	103	92	99	104	108	96	97	101	0.994005	995/1000	NonOverlappingTemplate
116	110	94	101	91	90	94	95	102	107	0.649612	984/1000	NonOverlappingTemplate
86	108	96	97	90	118	100	101	113	91	0.383827	992/1000	NonOverlappingTemplate
89	109	103	99	94	109	90	102	103	102	0.878618	993/1000	NonOverlappingTemplate
89	102	115	104	105	91	92	95	107	100	0.729870	993/1000	NonOverlappingTemplate
106	112	111	88	84	113	89	79	100	118	0.040635	990/1000	NonOverlappingTemplate
74	100	91	103	110	104	100	96	115	107	0.229559	993/1000	NonOverlappingTemplate
89	91	88	116	95	100	104	118	100	99	0.377007	991/1000	NonOverlappingTemplate
102	113	94	109	90	88	94	89	127	94	0.103753	990/1000	NonOverlappingTemplate
99	105	108	91	92	77	104	105	128	91	0.053627	992/1000	NonOverlappingTemplate
100	110	106	92	98	88	111	79	104	112	0.296834	989/1000	NonOverlappingTemplate
95	101	107	90	82	101	108	97	118	101	0.439122	994/1000	NonOverlappingTemplate
113	81	95	94	99	106	99	108	105	100	0.618385	985/1000	NonOverlappingTemplate
104	95	111	91	98	95	91	110	96	109	0.788728	987/1000	NonOverlappingTemplate
91	113	100	95	93	115	107	91	92	103	0.583145	990/1000	NonOverlappingTemplate
109	95	100	124	83	104	93	112	80	100	0.071177	990/1000	NonOverlappingTemplate
118	104	99	101	88	95	89	100	90	116	0.360287	986/1000	NonOverlappingTemplate
107	99	106	82	104	106	100	106	99	91	0.759756	990/1000	NonOverlappingTemplate
105	86	113	115	102	80	89	103	105	102	0.225998	994/1000	NonOverlappingTemplate
114	100	116	100	90	89	94	104	102	91	0.524101	982/1000	NonOverlappingTemplate
86	96	126	101	111	92	98	90	95	105	0.197981	996/1000	NonOverlappingTemplate
102	101	100	85	96	121	85	91	103	116	0.182550	986/1000	NonOverlappingTemplate
101	106	89	102	95	94	109	83	113	108	0.508172	989/1000	NonOverlappingTemplate
111	96	107	107	103	107	102	80	89	98	0.512137	989/1000	NonOverlappingTemplate
110	93	89	93	109	100	100	99	95	112	0.769527	988/1000	NonOverlappingTemplate
116	83	91	107	97	100	111	94	95	106	0.435430	988/1000	NonOverlappingTemplate
110	104	104	105	84	109	100	92	91	101	0.699313	995/1000	NonOverlappingTemplate
98	103	108	93	111	99	103	81	102	102	0.713641	986/1000	NonOverlappingTemplate
108	117	87	88	92	95	101	107	93	112	0.352107	988/1000	NonOverlappingTemplate
98	105	101	121	94	108	75	119	97	82	0.026057	991/1000	NonOverlappingTemplate
93	101	89	87	105	103	103	110	105	104	0.812905	988/1000	NonOverlappingTemplate
100	82	116	111	86	88	117	91	109	100	0.093157	984/1000	NonOverlappingTemplate
104	110	103	94	113	119	84	86	83	104	0.106246	993/1000	NonOverlappingTemplate
102	108	103	104	97	100	97	92	94	103	0.987896	994/1000	NonOverlappingTemplate
123	99	87	94	100	105	98	91	98	105	0.461612	987/1000	NonOverlappingTemplate
94	79	115	111	113	102	99	95	96	96	0.308561	988/1000	NonOverlappingTemplate
106	98	86	86	117	110	100	96	90	111	0.305599	992/1000	NonOverlappingTemplate
104	100	102	97	119	89	92	92	95	110	0.570792	989/1000	NonOverlappingTemplate
91	94	109	106	99	107	92	87	95	120	0.399442	990/1000	NonOverlappingTemplate
94	97	116	95	102	86	96	103	111	100	0.666245	991/1000	NonOverlappingTemplate
96	106	97	94	107	102	95	92	105	106	0.964295	985/1000	NonOverlappingTemplate
107	101	90	106	107	104	88	97	96	104	0.886162	986/1000	NonOverlappingTemplate
122	91	102	85	84	86	110	110	110	100	0.079051	990/1000	NonOverlappingTemplate
94	100	101	106	112	90	99	113	91	94	0.735908	983/1000	NonOverlappingTemplate
110	116	91	100	102	85	99	106	103	88	0.478839	991/1000	NonOverlappingTemplate
103	90	101	98	99	94	96	117	109	93	0.753844	992/1000	NonOverlappingTemplate
98	106	106	120	90	103	103	82	106	86	0.242986	992/1000	NonOverlappingTemplate
88	111	115	109	83	103	106	87	99	99	0.292519	982/1000	NonOverlappingTemplate
115	92	103	100	100	92	102	96	104	96	0.901959	987/1000	NonOverlappingTemplate
99	100	103	105	89	102	99	109	114	80	0.496351	987/1000	NonOverlappingTemplate
98	93	79	104	116	99	109	98	103	101	0.473064	991/1000	NonOverlappingTemplate
97	112	102	99	102	108	101	102	84	93	0.801865	993/1000	NonOverlappingTemplate

```
104 101  95  81 108 103  99  81 104 124  0.112047    989/1000    NonOverlappingTemplate
109  97 103 116 107 110  90  98  84  86  0.304126    988/1000    NonOverlappingTemplate
104  91 121 109 106  92  80  94  93 110  0.160805    984/1000    NonOverlappingTemplate
103  90  92  92 103  84 112 109 106 109  0.490483    990/1000    NonOverlappingTemplate
116  93 104  97 108  89  89  88 106 110  0.422638    994/1000    NonOverlappingTemplate
102 102 113 106 105  79 104  85 101 103  0.410055    989/1000    NonOverlappingTemplate
 93 124 100 104 101  97  96 106  86  93  0.394195    995/1000    NonOverlappingTemplate
104  72  95  99 100 110 110 103  95 112  0.211064    991/1000    NonOverlappingTemplate
 98  86 103 100 109  91 105  84 113 111  0.399442    986/1000    NonOverlappingTemplate
104 101 107 102  95  98 105 106  95  87  0.939005    988/1000    NonOverlappingTemplate
105  98 121 107  75  96 102  94 113  89  0.093720    987/1000    NonOverlappingTemplate
 93 116  92  93  98 108 103 110  88  99  0.595549    991/1000    OverlappingTemplate
118  97 110 102  99 100  97  95  79 103  0.417219    980/1000    Universal
 96  92  92 113  93 111 107  96 102  98  0.783019    988/1000    ApproximateEntropy
 67  65  67  55  69  71  58  60  54  57  0.779497    616/623     RandomExcursions
 53  61  44  73  80  88  48  57  48  71  0.000153    617/623     RandomExcursions
 69  52  47  65  83  55  57  64  58  73  0.052642    620/623     RandomExcursions
 71  58  71  65  61  54  62  71  61  49  0.522810    614/623     RandomExcursions
 58  56  52  67  59  72  54  65  76  64  0.435787    616/623     RandomExcursions
 65  53  65  72  56  67  64  54  77  50  0.259489    615/623     RandomExcursions
 71  63  62  53  81  48  49  68  59  69  0.069976    617/623     RandomExcursions
 62  73  56  63  64  55  74  65  61  50  0.513162    617/623     RandomExcursions
 56  65  54  60  64  60  70  52  73  69  0.601900    616/623     RandomExcursionsVariant
 64  55  48  69  60  65  64  62  67  69  0.712193    620/623     RandomExcursionsVariant
 59  61  47  76  62  68  67  59  54  70  0.338862    619/623     RandomExcursionsVariant
 62  60  53  65  73  62  70  59  70  49  0.494076    619/623     RandomExcursionsVariant
 61  58  66  62  67  60  74  67  56  52  0.747962    619/623     RandomExcursionsVariant
 60  65  76  56  60  54  73  65  56  58  0.535772    618/623     RandomExcursionsVariant
 58  71  70  75  63  62  63  54  50  57  0.426918    618/623     RandomExcursionsVariant
 65  67  61  66  51  72  67  68  53  53  0.535772    617/623     RandomExcursionsVariant
 57  70  55  59  63  67  58  61  79  54  0.459900    616/623     RandomExcursionsVariant
 56  55  64  65  67  63  53  63  68  69  0.860163    615/623     RandomExcursionsVariant
 64  54  66  63  60  52  61  60  72  71  0.735066    615/623     RandomExcursionsVariant
 75  64  66  45  55  59  71  64  61  63  0.346582    616/623     RandomExcursionsVariant
 83  62  54  62  66  54  58  64  56  64  0.318838    617/623     RandomExcursionsVariant
 74  66  66  62  49  69  52  66  57  62  0.472198    618/623     RandomExcursionsVariant
 63  69  70  59  62  54  64  48  72  62  0.548839    616/623     RandomExcursionsVariant
 63  62  63  71  56  59  73  58  54  64  0.800846    615/623     RandomExcursionsVariant
 58  74  56  61  75  61  71  55  44  68  0.128778    611/623     RandomExcursionsVariant
 64  63  52  77  67  59  69  58  58  56  0.558699    610/623     RandomExcursionsVariant
118 113 110  80 102 106  88  93  88 102  0.131879    987/1000    Serial
122  93 111 100  98  92 108  98  90  88  0.323668    986/1000    Serial
108  99  91 103  97  96 106 115  98  87  0.725829    988/1000    LinearComplexity


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 980 for a
sample size = 1000 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately = 609 for a sample size = 623 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Appendix B

Appendix B.1 NIST Statistical Test Suite ~ STS2.1.2 ~

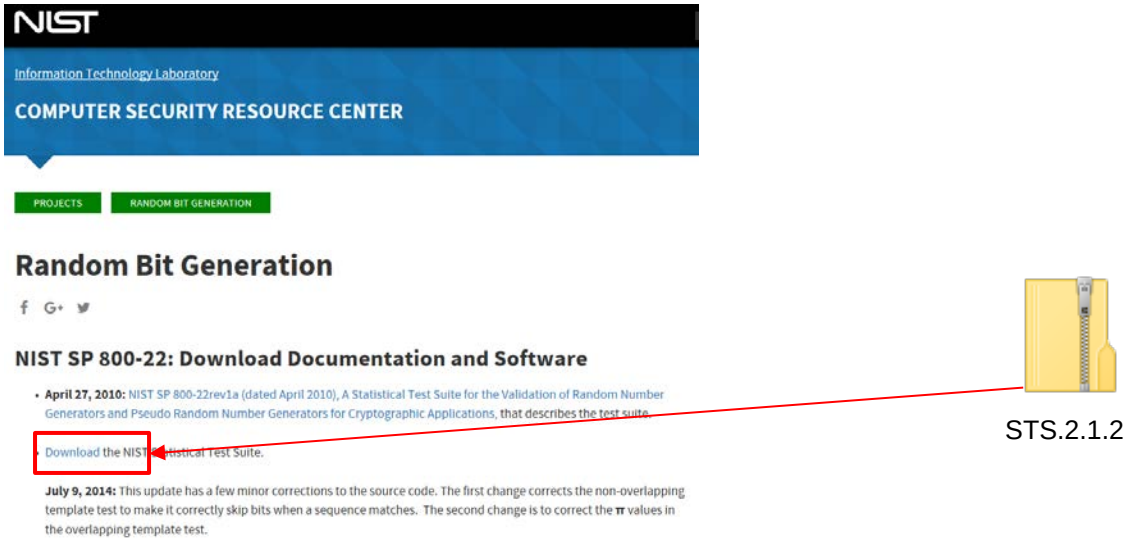
The **[SP800-22]** compliant test suite (**[STS2.1.2]**) is provided by NIST.

【Download page】

https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software

【File link】

https://csrc.nist.gov/CSRC/media/Projects/Random-Bit-Generation/documents/sts-2_1_2.zip



【File format】

Provided in C source files (public domain). Make command required for obtaining the test executable file.

【Operating environment】

Unix/Linux PC, or Windows PC with some compatibility layers like Cygwin, WSL.

gcc, make, and perl packages are also required.

【Test contents】

The 15 tests listed below and defined in **[SP800-22]** are executed:

- The Frequency (Monobit) Test
- Frequency Test within a Block
- The Runs Test
- Tests for the Longest-Run-of-Ones in a Block
- The Binary Matrix Rank Test
- The Discrete Fourier Transform (Spectral) Test
- The Non-overlapping Template Matching Test
- The Overlapping Template Matching Test
- Maurer's "Universal Statistical" Test
- The Linear Complexity Test
- The Serial Test
- The Approximate Entropy Test,
- The Cumulative Sums (Cusums) Test
- The Random Excursions Test
- The Random Excursions Variant Test.

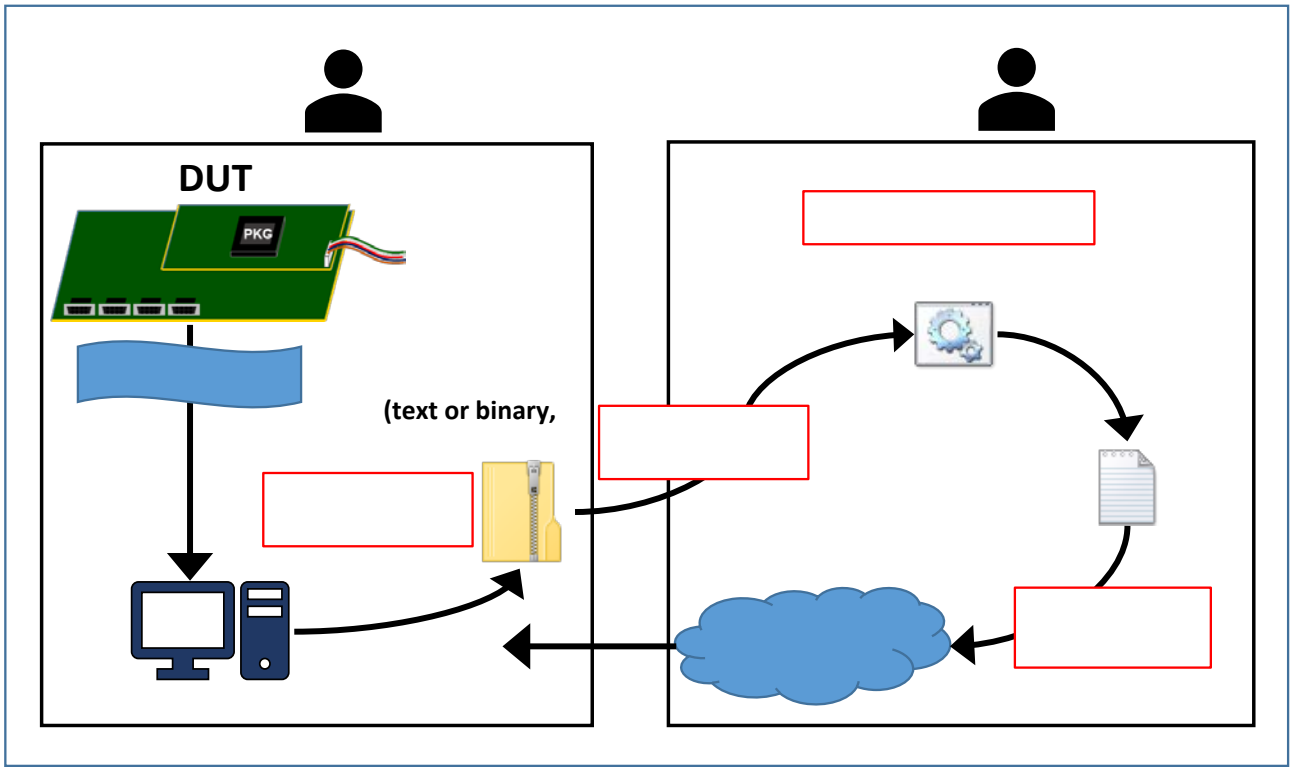


Figure 1. Random Number Evaluation Flow

① The client department runs the RNG on the target product and gains random sequences. The sequences are saved in a hexadecimal text format as the evaluation sample.

② The client department send the evaluation sample to the evaluation department.

③ The evaluation department evaluate its randomness with **[STS2.1.2]**.
(A) Convert the evaluation sample(②) into the single binary file.
(B) Run **[STS2.1.2]** with the “Sequence size” 1,000,000 bit in the argument.
(C) In the configuration “Input file”, select the binary file converted at (A).
(D) The tool will ask the “Sample size”, then specify 1000 samples.
(E) Other options are not changed from the default values.
(F) The test log “finalAnalysisReport.txt” is output to the experiments/AlgorithmTesting subdirectory.

④ The evaluation department checks each part in the test log described in Figure 2 and judges the Pass/Fail.
(A) Check the pass criteria of the Non-random excursion tests (C1 in Figure 2).
(B) Check the pass criteria of the random excursion tests (C2 in Figure 2).
(C) Check the pass proportion of the Non-random excursion tests (A1 in Figure 2) and the random excursion tests (A2 in Figure 2).
(D) If all the A1 and A2 values are greater or equal than C1 and C2 respectively, the test result is PASS.

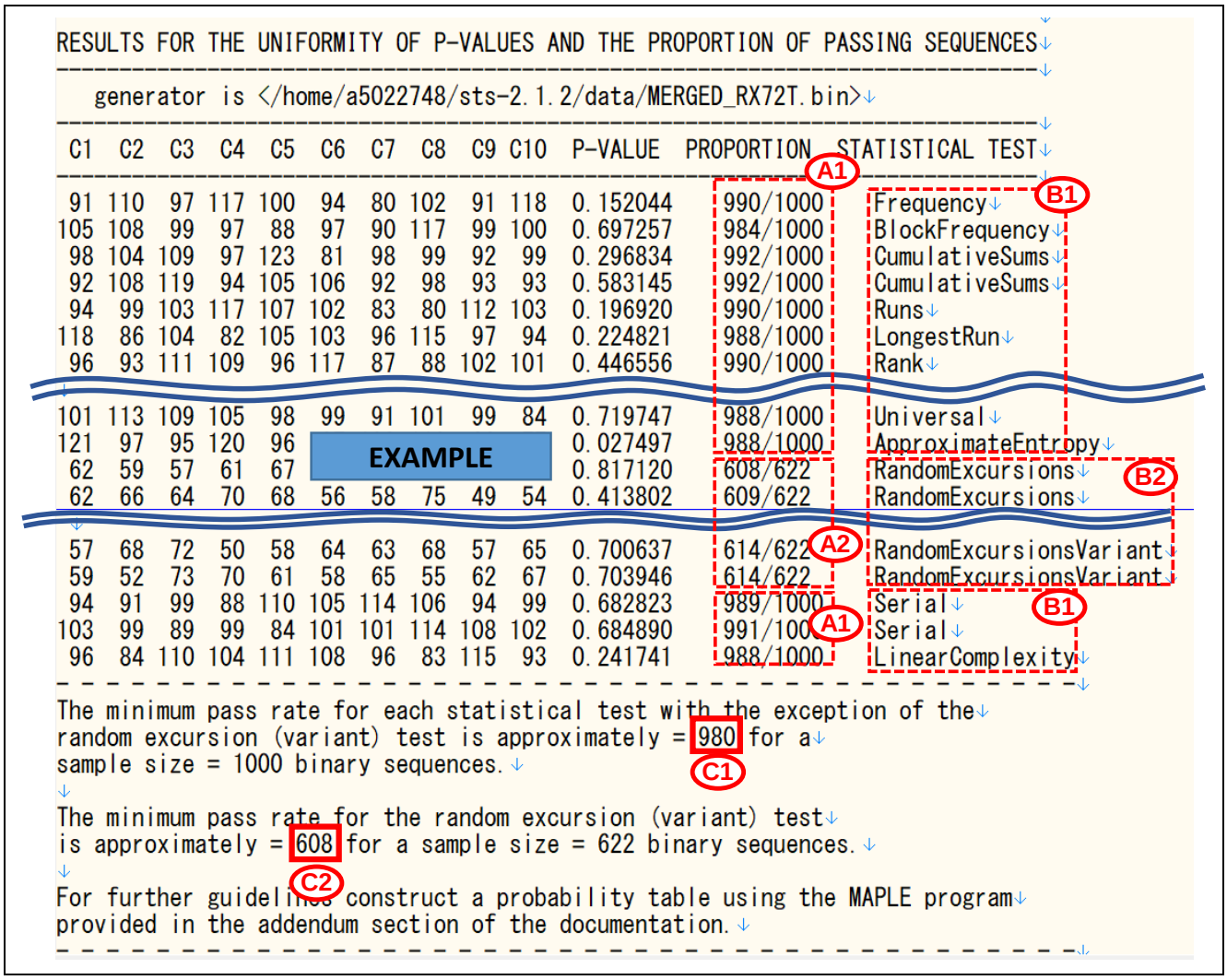


Figure 2. Descriptions in finalAnalysisReport

4. Website and Support

Visit the following URLs to learn about key elements of the RA family, download components and related documentation, and get support:

RA Product Information	renesas.com/ra
RA Product Support Forum	renesas.com/ra/forum
RA Flexible Software Package	renesas.com/FSP
Renesas Support	renesas.com/support

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Jul.26.23	—	Initial release

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.
(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.