

General

HG400 series non-deterministic random number (or random bits) generators are based on the effect of the electronics noise present in Zener diodes. Produced bits are virtually free of bias and correlations and independent of each other. Their main feature of these generators is non-determinism meaning that they can not accept any seed or initial state that would determine future output and that it is not possible to control or predict their output.

The noise is sum of two processes: **quantum tunneling** and **micro plasma avalanches**. Both processes are random, unpredictable and largely insensitive to environmental or electromagnetic influences. The noise is amplified and digitized. Digital pulses are then processed according to our patented method in order to produce random bits one at a time. HG400 series consist of 8 independent non-deterministic random bits generators which are combined to produce one whole byte at each sampling.

The maximum rate of production of random bits depends on the speed of electronic components and characteristics of the Zener diodes. There is a clear tradeoff between speed and price. In order that our customers can choose the optimum speed and price that best suits their applications, we offer a range of speed grades of the HG400 generators. Current models include **16 Megabit/sec** (HG416), **24 Megabit/sec** (HG424) and **32 Megabit/sec** (HG432).

OEM port

OEM port is realized with a 10-pin IEC jack and can be used for the serial output of the random bits and powering of the unit. With the OEM port a HG400 generator can be used as a standalone unit in applications which do not require the USB2.0 interface. One can read random bits at a full device speed from the OEM port.

The outputs are standard 5V CMOS compatible and can be used to directly drive 74HC, 74AC and 7LVC family logic.

Random data appear at the OEM port in the serial manner. There are three output lines (outputs): **Data**, **Clock** and **Strobe**. At each positive going edge of the Clock the corresponding Data value (logic 0 or 1) is already present at the Data output (see Fig. 1). Furthermore, the Strobe pulse appears just after every eighth Clock and can be used to trigger the data latching in a serial-in-parallel-out shift register, as shown on the Fig 2. If the standard 10-wire flat computer cable is used (Fig 3) it is important that the serial terminating resistances of 100 Ohm are deployed, or a devastating "ringing" may occur and deteriorate both the speed and the randomness quality. Fig. 1 shows the timing diagram of the three outputs, as measured at the end of 20 cm long flat cable with 100 Ohm serial termination.

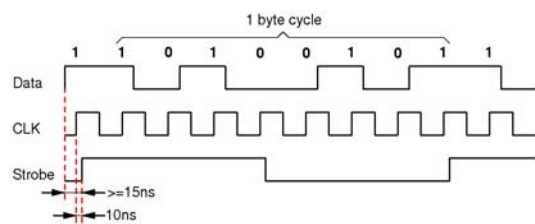


Fig. 1. Timing diagram of HG400 random number generators OEM port

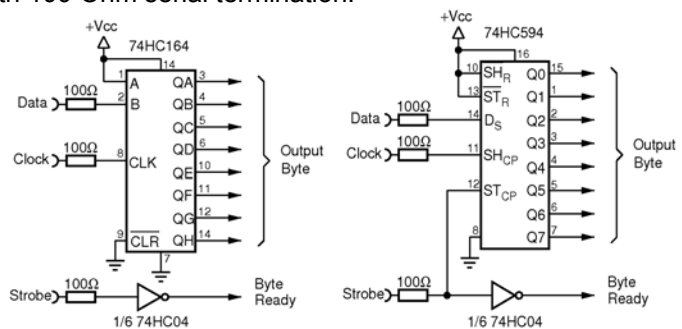


Fig. 2. Unlatched (left) and latched (right) examples of serial-to-parallel conversion for HG400 random number generators



Fig. 3. OEM port cable

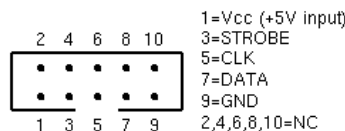


Fig. 4. OEM port IDC 10-pin connector pinout