Araneus Alea I

True Random Number Generator

User's Guide

Version 2.5

Introduction

The Araneus Alea I is a compact, high quality true random number generator with a USB interface. This User's Guide provides installation and usage instructions for users of Microsoft Windows, Linux, or NetBSD. The Linux and NetBSD instructions also apply to other Unix-like operating systems that have a generic USB device driver and/or **`libusb`**.

System Requirements

- ✓ One available USB 1.1 or 2.0 port
- ✓ A supported operating system

Supported Operating Systems

The Alea I supports the following operating systems:

- ✓ Windows XP (32-bit only, Service Pack 2 or newer required)
- ✓ Windows Server 2008
- ✓ Windows Vista
- ✓ Windows 7
- ✓ Windows 8
- ✓ Linux
- ✓ NetBSD
- ✓ any Unix-like operating system with **`libusb`** support

Both x86 (32-bit) and x64 (64-bit) versions of Windows Server 2008, Windows Vista, Windows 7, and Windows 8 are supported. IA-64 (Itanium) versions of Windows are not supported.

Using the Alea I with Windows

Using the Alea I with Windows requires installing a device driver using the driver CD provided. The driver CD also contains a simple example application to demonstrate how to use the driver, in both source and executable form.

Windows Software Installation

To install the Windows software for the Alea I, begin by inserting the driver CD into your CD-ROM drive. Do not attach the Alea I device to a USB port at this time.

The driver CD is set up to start the Windows software installer automatically when inserted. If this doesn't happen, for example if you have disabled the Windows AutoRun function, you can instead open the CD as a folder in Windows Explorer and double-click on the file **`setup.vbs`**.

You will be guided though the installation by a series of dialogs. You will be given the opportunity to customize the installation by selectively enabling or disabling the following components:

- ✓ Device driver
- ✓ Randomfile.exe example program
- ✓ Randomfile.exe C++ source code
- ✓ ActiveX control
- ✓ ActiveX examples

By default, all the components will be installed.

On 64-bit versions of Windows, both 32-bit and 64-bit versions of the ActiveX control are available. The 32-bit control will be used by 32-bit applications, and the 64-bit control will be used by 64-bit applications. By default, both versions of the control are installed.

During the installation, you may encounter pop-up dialogs requesting your permission to continue with the installation. If this happens, select the option to proceed with the installation.

Once the installer has completed, insert the Alea I device into a USB port. It may take Windows some time to recognize the newly plugged-in device and finalize the driver installation. On some versions of Windows, a *Found New*

Hardware Wizard window may pop up at this point. If so, respond to the question “Can Windows connect to Windows Update to search for software?” by selecting “No, not this time”, and to the question “What do you want the wizard to do” by selecting “Install the software automatically (Recommended)”.

Running `randomfile.exe`

The driver CD contains an example program **`randomfile.exe`** which reads random data from the Alea I and outputs it to the standard output stream.

To verify that the Alea I is operating correctly, you can open the folder **`\windows\examples`** on your CD-ROM drive and double-click on the **`randomfile`** icon. A window will appear, displaying a stream of random hexadecimal characters. To quit the program, click on the window close button.

If selected during the install process, the **`randomfile.exe`** program will also be installed to your hard disk as **`Program Files\Araneus\Alea\Examples\randomfile.exe`**.

For more detailed information on the use of **`randomfile.exe`**, please refer to the section titled *Using the randomfile program*.

Using the example C++ source code

The directory **`\windows\examples\source`** on the driver CD contains the source code for the **`randomfile`** program. If selected during the install process, it will also be installed to your hard disk as **`Program Files\Araneus\Alea\Examples\Source`**. The file **`ReadMe.txt`** contains instructions on how to build **`randomfile.exe`** from this source code.

The **`randomfile`** source consists of two C++ source files: **`randomfile.cpp`** is the randomfile program itself, and **`alea.cpp`** contains library code to simplify interfacing to the device driver. The interface to the code in **`alea.cpp`** is declared and documented in the header file **`alea.h`**.

If you wish to read random data directly from the Alea I in your own C++ application, copy the **`alea.cpp`** and **`alea.h`** files into your own source tree, **`#include`** the **`alea.h`** header file in your program, and link your program with the library **`setupapi.lib`**. See the comments in the **`alea.h`** header file for more details.

Please note that the device driver installed by version 2.0 or newer of the Driver CD is not compatible with C++ applications based on the example code shipped with driver CD versions earlier than 2.0. Applications based on the example source code included on this driver CD will work with all versions of the device driver, including ones older than 2.0.

Using the ActiveX Control

The Alea I ActiveX control allows the Alea I to be accessed from any Windows application or programming language that supports COM. For more information about using the ActiveX Control, please see the examples and **ReadMe.txt** file in the **\windows\activex\examples** directory on the driver CD. If selected during the install process, these files will also be installed to your hard disk as **Program Files\Araneus\Alea\ActiveX\Examples**.

Using the Alea I with Linux

Under Linux, the Alea I can be used by means of the **libusb** library without having to install any device-specific drivers. The directory **/linux** on the driver CD contains source code for an example program, **randomfile**, which reads random data from the Alea I using **libusb** and outputs it to standard output.

To build the **randomfile** program, create a new directory on your hard disk, **cd** to it, copy the files from the **/linux** directory on the driver CD to it, and type **make**.

To run the **randomfile** program, you need to either be **root** or have permission to open the device node of the Alea I as a non-root user. The way such permission is configured varies between Linux distributions. For example, on Ubuntu, you need to set up a **udev** rule by creating a file

/etc/udev/rules.d/50-araneus.rules

containing the two lines

```
# Araneus Alea I TRNG
SUBSYSTEM=="usb", ATTR{idVendor}=="12d8",
ATTR{idProduct}=="0001", MODE="0600",
OWNER="username"
```

replacing *username* with the actual username of the user who should be granted permission to use the device. Note that everything from **SUBSYTEM** onwards should be on a single line even if it has been broken into multiple lines above to fit on the page.

If you get the error message **unable to claim Alea interface 0**, it means you are missing the necessary permissions.

For detailed information on the use of the **randomfile** program, please refer to the section titled *Using the randomfile program*.

Using the Alea I with NetBSD

The NetBSD operating system has a built-in generic USB driver, **ugen**, that provides access to any USB device without the need to install a device-specific driver.

The simplest way to use the Alea I under NetBSD is to simply read from endpoint 1 of the **ugen** device. For example, the following shell command can be used to display random data on the screen in hexadecimal:

```
od -x </dev/ugen0.01
```

If you have multiple USB devices attached that use the **ugen** driver, you may need to replace **ugen0** with **ugen1** or a higher-numbered device.

The Alea I can also be accessed using the **libusb** library which is available as a NetBSD package (**pkgsrc/devel/libusb**). The directory **/netbsd** on the driver CD contains source code for an example program, **randomfile**, which reads random data from the Alea I using **libusb** and outputs it to standard output. For detailed information on the use of this program, please refer to the section titled *Using the randomfile program*.

Using the randomfile program

The **randomfile** program can be used to display random data on the screen, or its output can be redirected to a file for use by other applications or statistical analysis. It can be run from the command line (Unix shell or Windows command prompt).

The number of bytes of random data to generate is given as a command line argument. If no argument is given, an endless stream of random data is produced.

To store the random data in a file, redirect standard output using "**>**". For example, the command

```
randomfile 1000 >random.hex
```

writes 1000 bytes (8000 bits) of random data to the file **random.hex** as hexadecimal text. Note that since each byte of random data is represented as two hexadecimal characters, the resulting file will be 2000 bytes long.

To write raw binary data, specify the command line option **`-b`**. For example, the command

```
randomfile -b 1000 >random.bin
```

writes 1000 bytes (8000 bits) of random data to the file **`random.bin`** in binary form. The resulting file will be exactly 1000 bytes long.

USB protocol

This section contains information for advanced users who wish to develop their own drivers.

The USB protocol of the Alea I is straightforward. There is a single interface, interface 0, with a single bulk endpoint, endpoint 1. The random data are read from this endpoint in binary format using a packet size of 64 bytes.

The device may be identified using the USB Vendor ID and Product ID fields of the USB device descriptor. The vendor ID of the Alea I is 12D8 hex (4824 decimal) and the product ID is 0001 hex (1 decimal).

Specifications

- ✓ Random data rate: 100 kilobits / second typ.
- ✓ Interface: Full speed USB
- ✓ Power consumption: less than 250 mW
- ✓ Dimensions: 80 x 27 x 9 mm including the USB connector

Specifications are subject to change without notice.

Technical support

For further assistance, please contact us at alea-support@araneus.fi.