Interface between RTOS target and an Industrial System: Developing USB Digital I/O Module

Benjamin O’Brien

Embry-Riddle Aeronautical University

Graduate Research Project

3/22/13

Revision 0.1

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Signature** | **Date** |
| **Student** | Benjamin O’Brien |  |  |
| **GRP Advisor** | Dr. Andrew Kornecki |  |  |
| **MSE Coordinator / Department Chair** |  |  |  |
| **Reviewer** | Dr. Shou Pang |  |  |

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date** | **Revision** | **Description** |
| 3/22/13 | 0.1 | Initial Report Layout |
| 3/31/13 | 0.2 | Initial Content added |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table of Contents

[Table of Figures 4](#_Toc352509815)

[1 Introduction 5](#_Toc352509816)

[2 Objective 5](#_Toc352509817)

[3 Background 5](#_Toc352509818)

[3.1 Literary Exploration 6](#_Toc352509819)

[3.2 Existing Solutions 7](#_Toc352509820)

[3.2.1 Festo-Didatic EasyVeep 7](#_Toc352509821)

[3.2.2 Other Solutions (More on this later) 7](#_Toc352509822)

[4 Methodology 7](#_Toc352509823)

[4.1 Using EasyVeep 7](#_Toc352509824)

[4.1.1 Reversing the EasyPort Protocol 7](#_Toc352509825)

[5 Budget and Schedule 10](#_Toc352509826)

[6 Resources 11](#_Toc352509827)

[7 Appendices 12](#_Toc352509828)

[7.1 Reversing EasyVeep 12](#_Toc352509829)

# Table of Figures

[Figure 1: Proposed System Configuration 5](#_Toc352509830)

[Figure 1 : EasyPort Protocol Sequence Diagram 9](file:///C:\Users\zagi\SkyDrive\GRP\docs\worddoc\GRP_Report.docx#_Toc352509831)

[Figure 2 : EasyPort COM Port Discovery Code 13](#_Toc352509832)

[Figure 3 : EasyPort DCB Parameters 14](#_Toc352509833)

[Figure 4 : EasyPort.OCX Snippet Returning EasyPort Inputs 15](#_Toc352509834)

[Figure 5: EasyPort.OCX Snippet Storing Input Values 16](#_Toc352509835)

**Table of Tables**

[Table 1 : EasyPort Protocol Listing 8](#_Toc352509836)

# Introduction

This Graduate Research Project (GRP) was conducted in Spring 2013 at Embry Riddle Aeronautical University, under the supervision of Dr. Andrew Kornecki. The proposed area of research involves examining freely available real time industrial system simulation software and creating hardware device and supporting software necessary to allow students to control and interact with the simulated industrial systems. Such hardware and software would increase the number of systems with which the RTOS hardware targets could interact, allowing the Real-Time Systems (RTS) course students to gain more experience with controlling systems in real time.

# Objective

The main objective of this research is to construct a low-cost, working solution that will allow students taking the Real-Time Systems course to interact with and control system simulations provided by the EasyVeep software or a similar system. Currently only Festo’s proprietary EasyPort hardware is capable of interacting with the targeted software, but the EasyPort is an inadequate solution for various reasons detailed elsewhere in this report. Through various techniques including the analysis of available EasyPort specifications, inspection of system operation, and reverse engineering techniques it is possible to create a viable hardware and software solution to allow the RTOS target to interact with various system simulations.



Figure 1: Proposed System Configuration

# Background

The following sections include detailed descriptions of research that was performed during the proposal and initial development stages of the GRP. This section primarily documents the state of existing work in this field of study. This section also establishes the selected scope of work which is detailed in the Methodology section.

## Literary Exploration

The main motivation for this project was the discovery of the EasyVeep software. A major hurdle in achieving the objective of real time industrial simulation is creating accurate models. EasyVeep provides many already constructed simulations for free. The cost of the required EasyPort is a setback, however. Therefore before beginning a literary review was performed to determine if there was a more appropriate solution or a reasonably priced alternative to the EasyPort.

Initial research began using the IEEE Xplore database, which returned marginal results when searching for Festo and no results when searching for EasyVeep or EasyPort. The results found when searching for just Festo were more directed towards the use of Festo PLCs and other, non-free, simulation tools for use as training aids. The typical papers found that the tools were in fact quite useful for instruction, but published research into cheaper and more open source hardware options that work with the EasyVeep software was not found (Li, Lu and ZhiPing).

The search was expanded using Google Scholar. A conference paper was found discussing various software suites used for virtual training in control and automation. The author found that while there are various solutions, “All these tools require licensing whose price various according to the tool” and that EasyVeep was only one of a very few “final applications for practicing” control and automation (Izaguirre).This further reinforced the importance of basing the solution off of EasyVeep.

Since no moderately priced commercial solution was found, a search was performed to find similar academic projects. Limited information was found from a group called Fast Forward Technologies (Wolowicz and Knoll). The group was created as a result of a senior level design project at the University of Victoria to replicate an EasyPort. Their approach, however, was not to replicate the EasyPort exactly, but to create their own implementation that simply fit in the same form factor and used a USB interface instead of an RS232 serial interface (Wolowicz and Knoll). Their selected hardware and protocol were quite different from the EasyPort and most documents listed on their website were marked as proprietary. No further attempts to reverse engineer or replicate the EasyPort were discovered.

Most other literature found focused on simulating the control device instead of or in addition to simulating the processes. A well-documented design for a Virtual Plant Generator was found, but the paper didn’t provide any details on creating a hardware interface (Ngalamou). The Virtual Plant Generator was designed to use QT for simulation graphics, but it was mentioned that Flash, like EasyVeep uses, was a viable alternative. Another paper discussed extending PLC simulation software to interact with real world processes. Though the concept presented in the paper is exactly opposite of objective, some concepts could be considered useful. The solution used a parallel port but states clearly that the solution could be adapted to use serial or USB (ROMANIA). Some of the issues that could arise with such a system were documented as well.

The search continued for EasyPort like devices that could be modified to work with EasyVeep. More proprietary implementations of EasyPort like systems were found. Sealevel systems provides a wide range of Digital I/O USB solutions with up to 16 inputs and outputs (Sealevel). The units are industrial grade and use a proprietary SeaMAX protocol. The protocol used by the Sealevel units prevents them from being a viable solution to link the Real Time target to the simulated industrial systems, but the Sealevel website provides other valuable resources that can be applied to the propose project. Sealevel freely provides select chapters of its publication The Digital I/O Handbook which includes descriptions and design considerations for Digital I/O implementations (Sealevel).

## Existing Solutions

There are a number of existing simulation solutions for real time industrial control, but few come close to meeting the goal of this research project. Most available hardware and software solutions examined focus on training users to program and operate PLCs.

### Festo-Didatic EasyVeep

EasyVeep is advertised as a “graphical 2D process simulator with numerous attractive examples on PLC training.” EasyVeep is distributed freely and can be acquired easily. However, the software requires an external hardware interface, which is also produced by Festo-Didatic, called an EasyPort.

### Other Solutions (More on this later)

# Methodology

This section details the methods used and steps taken to complete the GRP. It is broken down into sections that coincide with the main work items that were experimented with during the research process. The items are presented in the chronological order in which they were researched.

## Using EasyVeep

As a software solution EasyVeep appears capable of meeting all the required functionality as discussed in Existing Solutions. In order to be used, a custom hardware device which replicates the behavior of Festo’s EasyPort is need. During in initial inspection of the manufacturer’s website, the documentation on the EasyPort was found to be inadequate in allowing complete replication of the EasyPort’s behavior. Eventually a document containing a protocol explanation was found after some broken links were fixed on Festo’s website. While waiting for the links to be repaired, a binary analysis of EasyVeep and its supporting binaries was performed.

### Reversing the EasyPort Protocol

The process of reversing the EasyPort protocol was a challenge. The extensive details on how the protocol was partially reversed are included in the appendix section Reversing EasyVeep. Primarily, the process consisted of static binary analysis using the freeware version of the Hex-Rays IDA interactive disassembler. Through examination of the files included with the EasyVeep installation, the library that facilitates serial communication with the EasyPort was located and analyzed both statically and dynamically.

To facilitated dynamic analysis, the com0com loopback driver was used to redirect, examine, and send information between various processes running on the local machine. This allowed for easy logging of the communication protocol as well as allowing fuzz testing of the library when attached to a debugger. Fuzzing was used when there was some ambiguity as to the content or context of the protocol. By attaching a small Python script to the other end of com0com loopback, simple EasyPort emulation was possible, and the data being sent back to the EasyPort library could be fuzzed until the desired debugging breakpoint was hit. A summary of the discovered protocol is shown in the table and figure below. This is an incomplete version of the entire protocol but includes all functionality necessary to meet the project objective. Commands are given in the format of a regular expression that would match a valid command. Each command is terminated with a carriage return.

Table 1 : EasyPort Protocol Listing

|  |  |
| --- | --- |
| Command Format | Description |
| setup0 | Request made by PC to initialize connected EasyPorts. |
| setup[1-4] | EasyPort response to setup0 command requesting a module number 1-4. |
| DV | Request by PC to get EasyPort version |
| V=\d.\d{2} | Response to version request containing the version number of the EasyPort. Must exceed (1.20). |
| MAW=[1-4].[0248]=[0-F]{4} | Modify the 16 bit output value of EasyPort module [1-4], channel log2([0248]) to be the value represented by hex number [0-F]{4}. |
| DEW[1-4].[0248] | Request the current input values from module [1-4], channel log2([0248]) |
| EW[1-4].[0248]=[0-F]{4} | Response to input value request. The current value of the inputs is represented by a four digit hex number. MAW command is sent in response. |

Figure 1 : EasyPort Protocol Sequence Diagram

EasyPort

Computer

COM Setup

Module Identification

Update Output

Update Input

setup0

setup1

DV

V=1.21

DEW1.8

EW1.8=0000

MAW1.0=0001

DEW1.8

EW1.8=0000

MAW1.0=0400

### Implementing an EasyPort

After determining the protocol that would be used, an attempt was made at implementing the EasyPort protocol on an Arduino Uno R3. The Arduino was selected for simplicity, and while it lacked the number of pins necessary to provide two full 16bit channels, it provided enough I/O to interact with a decent subset of the models provided by EasyVeep.

After implementing the startup protocol on the Arduino it was tested using the serial monitor included with the Arduino IDE. When typing commands into the serial monitor that coincided with the commands the Arduino would be receiving from EasyVeep the behavior was as expected. However, when EasyVeep attempted to talk to the Arduino the connection was not established. Modifying the Arduino program to blindly count received bytes instead of parsing the protocol allowed it to completely the connection process before failing.

The Arduino was behaving as if it was not receiving valid serial data from EasyVeep, but sending data to EasyVeep perfectly fine. At the time, access to a logic analyzer was not available, and after multiple re-writes of the serial processing code, the code was modified to log all bits received to the Arduino’s EEPROM and report them over the serial line the next time the Arduino reset. The EEPROM writes were required because the Arduino resets every time a new device connects to it, so it was the only way to keep the data persistent.

With the new code, the Arduino was connected to EasyVeep and sent two “setup0\r” commands. EasyVeep was then closed and the Arduino serial monitor was opened. The EEPROM was dumped and the values were found to all be hexadecimal FF. The number of bytes logged to EEPROM, however, was exactly the same as the number of bytes in two “setup0\r” commands. This showed that the Arduino was receiving serial data but all the received bits were ones.

After many hours of debugging, it was found that the Arduino does not support the Clear To Send (CTS) and Request To Send (RTS) flow control operations. EasyVeep was attempting to use proper serial flow control and as a result, it appears that the Arduino was receiving corrupted data. Since the Arduino uses a FTDI UART to USB IC, the IC only provide interfaces with the TX and RX pins and there is no way to enable flow control on the Arduino Uno.

With the Arduino eliminated as a valid platform, com0com was used to set up a loopback serial connection that supported flow control. A C# Windows Form Application was developed that provided a serial log window along with checkboxes to simulate changing inputs and a field to hold the current output value. Shortly after adding the protocol implementation to the form application end to end communication with EasyVeep was achieved.

# Budget and Schedule

# Resources

**There are no sources in the current document.**

Ngalamou

http://paper.ijcsns.org/07\_book/201009/20100908.pdf

Romanian

http://www.aece.ro/abstractplus.php?year=2010&number=1&article=15

Izaguirre

http://www.indiana.edu/~ciec2011/ETD/ETD-351/ETD-351\_Izaguirre.pdf

# Appendices

## Reversing EasyVeep

In order to begin the reversing process, information regarding the format and structure of the EasyVeep executable needed to be obtained. The analysis began by simply launching EasyVeep. The user is greeted with a “Made with Macromedia” splash screen and visiting the Setup pane in EasyVeep confirms that the software relies heavily on what was previously known as Macromedia Flash Player (now an Adobe product). This was helpful information, and Flash, from previous experience, was known to be easy to decompile and reverse engineer in comparison to binaries produced with languages such as C and C++. However, pure Flash based programs cannot directly communicate with low level system devices such as serial ports; there are no documented functions in the official documentation for doing so. This indicates that the functionality of interest resided elsewhere. Analysis indicates that EasyVeep uses Flash only for running and displaying the simulated processes. Communication and protocol implementation is handled elsewhere.

The next step in the analysis was to examine the EasyVeep executable more closely. The assembly information was examined by viewing the executable properties. It was found to be an Authorware Runtime application. Authorware is primarily designed for developing learning management systems (LMS) in a visual manner (INSERT SOURCE). Given the description of the Authorware software, it did not appear that the Authorware application itself would have access to the serial port but further analysis was needed to eliminate the main executable as the targeted binary. To do so the Import Address Table (IAT) of the EasyVeep module was inspected.

The IAT serves as a table of virtual function pointers to various functions encapsulated in external libraries (<http://sandsprite.com/CodeStuff/Understanding_imports.html>). If the EasyVeep application were to perform the serial communication itself, it would likely be importing serial control functions from the Windows API. After dumping the IAT for EasyVeep.exe the 457 entries were checked and none appeared to have anything to do with serial communication. Additionally, the strings list was checked as well for anything related to serial communication. The strings table holds a list of all the ASCII strings used by a program and in this case, nothing related to the windows COM port file descriptor (\\COM%d) used when opening a serial port was found.

After the search for serial port related functions failed to turn up anything significant, the IAT was examined again for clues on where to look direct attention to next. Most imports were from the GDI32 library (Graphics Device Interface), USER32, and KERNEL32 libraries. The USER32 and GDI32 imports all were directed towards drawing and presenting the user interface while the KERNEL32 library functions were reading and traversing file directories and processes. The imports the proved to be of interest were those from the ole32 library. The ole32 library implements Object Linking and Embedding (OLE) which is primarily used for embedding and linking disparate data items, such as embedding a Flash movie into a Microsoft Word document. The OLE allows developers to create their own OLE Control Extensions (OCX) to extend functionality of existing user interfaces.

Inspection continued of the OLE functions. Using the freeware version of IDA interactive disassembler, breakpoints were set on all functions that loaded OLE objects. However, when launching the application through the debugger, exceptions were thrown and the application refused to load and hit the breakpoints. Instead of attempting to debug further, as bypassing anti-debugging measures is not within the extent of this project, a different approach was taken. EasyVeep was launched without a debugger attached and then once fully loaded IDA was used to attach the debugger. IDA provides a list of loaded modules and within that list a module named EasyPort.ocx was found. This appeared to be a promising target as it was named after the device that was being reverse engineered.

The EasyPort.ocx file was loaded into IDA for disassembly and debugging. Immediately upon checking the IAT, functions GetCommState, BuildCommDCBA, SetCommState, and PurgeComm appeared at the top of the list. A quick Google search showed that these were all part of the Windows Communication Functions API (<http://msdn.microsoft.com/en-us/library/windows/desktop/aa363194(v=vs.85).aspx)>.

The COM functions were break pointed and the debugger was attached to a running EasyVeep process. By stepping through the process it was found the EasyPort.ocx begins iterating over a range of integers, attempts to open a COM port of that integer, and then establish communications with an EasyPort device. The COM initialization code is shown below.



Figure 2 : EasyPort COM Port Discovery Code

This code first builds the file description string for the COM port and then builds the DCB control settings for the serial device. It then tries to open the COM using CreateFileA and the commands immediately following that function call attempt to detect and report errors. A breakpoint was set after the third sprint call to examine the string that was used setting the DCB for the serial device. It was found that for each COM port, the above routine gets called twice. The first time a baud rate of 19200 is used and the second time a baud rate of 115200 is used. If communication fails on both baud rates, the next COM port is tried until no more remain. If communication success, the process continues and all ports found to have a COM device are reported to EasyVeep.



Figure 3 : EasyPort DCB Parameters

To determine if the COM port is attached to an EasyPort, the EasyPort.ocx sends the ascii string “setup0\r” and waits for a response. If a response is not sent in a valid time frame the setup string is sent again. In return, the software expects a string in the format of “setup%1d\r” to be returned where the value represented by %1d is between 1 and 4. If this succeeds, the string “DV\r” is sent. The expected string in return is in the format of “V=%1d.%2d\r”. Once this exchange is complete, the validity of the EasyPort is confirmed.

Upon getting a list of valid COM ports, EasyVeep will attempt to open each in order to determine what variation of EasyPort they are. It does this by sending the message in the form of “DEW%d.8” where %d corresponds to the number received from the EasyPort during the setup process. It appears that the length of time and manner in which the EasyPort responds to these requests effects the model type returned. Further analysis has not been made, as it was found during implementation that simply responding as fast as possible would cause the emulated EasyPort to be returned as the correct type.

Further analysis was performed on the OCX object to determine what occurs after setup. It was recognized that the OCX was in the same format as a typical windows com object, so the virtual method table (vtable) was located in the .rdata section of the EasyPort.ocx disassembly (<http://blogs.msdn.com/b/oldnewthing/archive/2004/02/05/68017.aspx>). The vtable holds the name of the methods that can be called from a process using the OCX along with pointers to the associated functions. This allows plain text, expressive function names to be used in deciphering the cryptic disassembly.

The vtable contained many more methods than were necessary for meeting the project objective, so only those that were of concern were examined. The first function examined was “SetOutput”. The trace for set output eventually led to the sending of a command “MAW%d.%1d=%04X”, where MAW seemed to stand for Modify Output Word. The %d.%1d was similar to the “DEW%d.8” command found earlier, where the first digit corresponded to the module number, thus the format is Module#.Channel# = HexValue.

Determining how the input values were obtained was not as straight forward. The “GetInputWord” function did not directly lead to a certain serial command, but instead a small move instruction. The move instruction references an address based around the ecx register, which in C++ typically holds the address of the “this” variable. Therefore, at [eax\*4+0x24], the value of the most recent input is stored, where eax is assumed to be the module number.

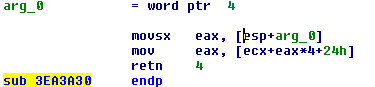


Figure 4 : EasyPort.OCX Snippet Returning EasyPort Inputs

Examining the code the is run when a serial data stream is received eventually led to a case where an almost identical, but reversed move was found. The same offset is being used to load the effective address of the field into edx and then the value in eax is moved into the address pointed to by edx. This code was found by tracing the execution for the case when the serial input is of the form “EW%1d.%1d=%4X\r”. Here EW denotes the value of the input word is the included four digit hex number.

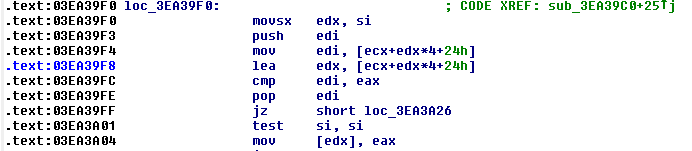


Figure 5: EasyPort.OCX Snippet Storing Input Values

With this knowledge, all the commands necessary to establish connection and interact with the base functions of EasyVeep are known. The cadance to initialize setup, along with the commands used to modify outputs, and query and update inputs are well documented. None of the other commands that a production EasyPort can interpret are necessary to perform the project objective.