Management had maintained that this was a serious application, and time should be spent improving the basic functionality rather than wasted on making it look pretty. After seeing the results, they changed their standard presentation of the system to highlight it.

So can X programming be done quickly? A look at the documentation can be discouraging. The standard documentation included with X is intimidating. It is a reference set, make no mistake, with few if any examples. The source code included with X can provide useful information, but it is generally not well enough commented to explain how X works. An excellent manual set is available from O'Reilly and Associates, but it consists of seven volumes (and counting). Is it necessary to read all of them? Where should you start?

The fact is, there is a significant learning curve before one becomes a competent X programmer. There is a lot of background material to cover. There are, however, a few hints that can save time and frustration.

Use Toolkits

This is a significant savings in and of itself. The tendency is to go directly to the XLib (lowest) level, because the calls are somewhat familiar to people who have done graphics-oriented programming in the past. The problem with this approach is the sheer effort involved in reproducing the functionality of currently available high-level toolkits. The exception to this rule might be a systems programmer, who would be doing low-level X programming for a group of high-level programmers. It often helps to have somebody around who understands the underlying system, but it would be difficult to justify the time to bring an entire programming group up to speed.

Write Event-Driven Programs

The natural tendency is to attempt to use traditional programming techniques, forcing the X system to do what the program wants when it wants it done, usually in an orderly, sequential manner. X applications work best when they are structured as a series of small, self-enclosed routines that react to events. These routines should have minimal interdependence, so that a change in the order or timing of events doesn't affect their functionality. This programming model is very object-oriented (isn't everything these days?), and thereby can gain the advantages promised by that crowd, notably resuability, maintainability, and all those other wonderful -ilities. Interestingly enough, I think some of the best training for this model of programming is working on interrupt-driven device drivers, giving many embedded systems programmers an advantage.

CONCLUSION

X Windows is a significant event in the programming world, cutting across a wide range of fields. Embedded systems is potentially one of the areas that can benefit, but that depends on whether the practitioners of the field will use the new tools that are available. It is often difficult to break away from the day-to-day grind of short deadlines, but X and other new technologies have much to offer in return for the investment.

Larry Mittag is an independent consultant specializing in real-time embedded systems. He has 12 years' experience in the field and is a contributing editor to Embedded Systems Programming.
INTRODUCTION

Programming for embedded systems has always been complicated by the difficulty of debugging embedded code in restricted hardware environments, at least in comparison to most PC or workstation environments. It is possible, though, to leverage debugging efforts by utilizing hardware on the target, as well as tools generally found in a hardware or systems development lab. In this paper, I will describe some techniques for utilizing various types of hardware to help ease the software debugging burden.

DEFINING THE PROBLEM

Debugging can be thought of as a search for information. The primary questions to be answered include determining what the code is doing at any given time, how it got to a certain point, and how long it takes to perform an operation or set of operations. The basic difficulty in answering these questions with embedded systems is that there is normally less I/O capability available. Couple this with tight timing constraints, and the result can be a debugging nightmare.

Attempts to utilize limited I/O capabilities such as serial ports for debugging purposes are at their best difficult. At worst, a sort of Heisenberg Uncertainty Principle occurs, where the attempts to characterize the behavior of the system has distorted that behavior to the point where the information obtained may be useless. This is especially apparent when debugging real-time behavior.

The goal is therefore to use noninvasive means to obtain information about the system. Any software utilized for this purpose that uses the target system resources will inevitably perturb the system, so we will explore other means.

DEBUGGING AIDS ON THE TARGET HARDWARE

It is remarkable how much information can be obtained if the target system itself is designed to facilitate software debugging. Addition of some LED’s and a register to control them provides a low overhead (in terms of added code) means to determine the health of embedded code. The most obvious use of this is a “heartbeat” indication, allowing easy determination of whether a board has died.

An example of this is the front panel that used to be found on minicomputers, with LED’s continuously showing the state of the address and data lines. An experienced operator could tell at a glance whether the system was operating normally, as well as getting a feel for how heavily loaded it was, since they often ran a certain pattern when the CPU was in its idle loop.

An LED display can help in postmortem situations, also. It is downright rude when a system goes down with no indication as to the cause of death. An error code displayed by an LED register might be just the message from beyond the grave needed to solve the problem.

It is possible to build more sophisticated debugging aids onto target systems, but it is often not worth it. Beyond the additional cost, such systems are often more prone to failure than the hardware itself. A better approach is to have the hardware engineer spend time bulletproofing the core hardware, and then add some simple debugging aids such as LED’s to assist software developers. In general, simpler is better.

Some more esoteric debugging aids may come “free” though, since they are beginning to be integrated into popular microprocessors. The debug registers in the Intel i386 are a good example, allowing breakpoints and some other emulator functions to be implemented without the need for additional hardware. Another noteworthy addition is the software watchdog timer on the Motorola 683XX line, which automatically causes an interrupt if a certain register is not accessed at regular intervals. This can be used to restart fault-tolerant systems or to trigger a postmortem dump which may provide clues as to the cause of death.

The advantage to debugging aids built onto the target hardware are that they are always available. They can be used to debug during system development, as well as after the system is in the field. The disadvantage is that they may add to the cost and complexity of the system being developed and they often do not provide enough information to solve tough problems. This is when use of external debugging hardware is appropriate.

EMULATORS

The first piece of external equipment most programmers will turn to is an In-Circuit Emulator (ICE). This is logical, since a useful ICE will provide an environment similar to a good symbolic debugger, allowing a very high degree of visibility and control of the target code. Using an ICE to single-step through code and examine variables and registers is almost the definition of debugging for many programmers.

Unfortunately, most programmers never look beyond that. An ICE should be thought of more as a set of resources that are temporarily being loaned to the target system, allowing the programmer to do things they couldn’t otherwise do. A good example of this was a problem I was recently called in to solve.

A particular target system was experiencing a variety of flaky errors. Code that ran fine on other systems would act differently on this one, up to and including experiencing fatal errors. Any change in the code to add diagnostics to isolate the problem would change the behavior, often making the problem go away completely.

I suspected hardware problems, but it was difficult to determine exactly what the nature of the problem might be. The hardware engineer who had designed the prototype board was in Taiwan, so consultation was expensive if not impossible. I left instructions that I was to be called when a fatal error occurred on that system, and that once it happened no one was to
INTRODUCTION

Programming for embedded systems has always been complicated by the difficulty of debugging embedded code in restricted hardware environments, at least in comparison to most PC or workstation environments. It is possible, though, to leverage debugging efforts by utilizing hardware on the target, as well as tools generally found in a hardware or systems development lab. In this paper, I will describe some techniques for utilizing various types of hardware to help ease the software debugging burden.

DEFINING THE PROBLEM

Debugging can be thought of as a search for information. The primary questions to be answered include determining what the code is doing at any given time, how it got to a certain point, and how long it takes to perform an operation or set of operations. The basic difficulty in answering these questions with embedded systems is that there is normally less I/O capability available. Couple this with tight timing constraints, and the result can be a debugging nightmare.

Attempts to utilize limited I/O capabilities such as serial ports for debugging purposes are at best difficult. At worst, a sort of Heisenberg Uncertainty Principle occurs, where the attempts to characterize the behaviour of the system has distorted that behaviour to the point where the information obtained may be useless. This is especially apparent when debugging real-time behaviour.

The goal is therefore to use nonintrusive measures to obtain information about the system. Any software utilized for this purpose that uses the target system resources will inevitably perturb the system, so we will explore other means.

DEBUGGING AIDS ON THE TARGET HARDWARE

It is remarkable how much information can be obtained if the target system itself is designed to facilitate software debugging. Addition of some LED's and a register to control them provides a low overhead (in terms of added code) means to determine the health of embedded code. The most obvious use of this is a "heartbeat" indication, allowing easy determination of whether a board has died.

An example of this is the front panel that used to be found on minicomputers and microcomputers, with LED's continuously showing the state of the address and data lines. An experienced operator could tell at a glance whether the system was operating normally, as well as getting a good feel for how heavily loaded it was, since they often ran a certain pattern when the CPU was in its idle loop.

An LED display can help in postmortem situations, also. It is downright rude when a system goes down with no indication as to the cause of death. An error code displayed by an LED register might be just the message from beyond the grave needed to solve the problem.

It is possible to build more sophisticated debugging aids onto target systems, but it is often not worth it. Beyond the additional cost, such systems are often more prone to failure than the hardware itself. A better approach is to have the hardware engineer spend time bulletproofing the core hardware, and then add some simple debugging aids such as LED's to assist software developers. In general, simpler is better.

Some more esoteric debugging aids may come "free" though, since they are beginning to be integrated into popular microprocessors. The debug registers in the Intel i386 are a good example, allowing breakpoints and some other emulator functions to be implemented without the need for additional hardware. Another noteworthy addition is the software watchdog timer on the Motorola 683XX line, which automatically causes an interrupt if a certain register is not accessed at regular intervals. This can be used to restart fault-tolerant systems or to trigger a postmortem dump which may provide clues as to the cause of death.

The advantage to debugging aids built onto the target hardware are that they are always available. They can be used to debug during system development, as well as after the system is in the field. The disadvantage is that they may add to the cost and complexity of the system being developed and they often do not provide the enough information to solve tough problems. This is when use of external debugging hardware is appropriate.

EMULATORS

The first piece of external equipment most programmers will turn to is an In-Circuit Emulator (ICE). This is logical, since a useful ICE will provide an environment similar to a good symbolic debugger, allowing a very high degree of visibility and control of the target code. Using an ICE to single-step through code and examine variables and registers is almost the definition of debugging for many programmers.

Unfortunately, most programmers never look beyond that. An ICE should be thought of more as a set of resources that are temporarily being loaned to the target system, allowing the programmer to do things they couldn't otherwise do. A good example of this was a problem I was recently called in to solve.

A particular target system was experiencing a variety of flakey errors. Code that ran fine on other systems would act differently on this one, up to and including experiencing fatal errors. Any change in the code to add diagnostics to isolate the problem would change the behaviour, often making the problem go away completely.

I suspected hardware problems, but it was difficult to determine exactly what the nature of the problem might be. The hardware engineer who had designed the prototype board was in Taiwan, so consultation was expensive if not impossible. I left instructions that I was to be called when a fatal error occurred on that system, and that once it happened no one was to
touch anything until I arrived.

It took several days, but the call did come. The system was getting an illegal instruction trap at a particular address. I used the ICE to examine that address, seeing what was indeed an illegal instruction. The corresponding byte in the load module differed by a single bit. Changing the value to the correct one allowed the code to run correctly.

I took advantage of the extra memory provided by the ICE to load the code twice, once at the correct location and once at a higher base address. I then had the ICE compare the two areas. The bit had been set wrong only in the lower memory area. It turned out that there was a memory error that caused that bit to be overwritten when a location 4096 bytes away was set. If the two happened to be the same, no problem. If they differed, flakiness resulted. I used the ICE to remap that area into ICE memory instead of target, and all problems went away.

The key to full use of an ICE is to understand fully the degree of control it really does provide. ICE memory can be used to supplement a stingy target, allowing the addition of test routines to the code to assist debugging. Watchpoints can be set to determine what part of the code is overwriting sensitive memory areas. It is also a great tool for ad hoc testing of hardware, since values can be poked into registers and the values read back without the need for writing code.

The other necessity for effective ICE use is to understand what it will not do. Vendor claims can lead you to assume that system behaviour under ICE control is exactly as it is when the ICE isn’t installed. I tend to treat this as a pleasant surprise when it occurs, but generally don’t count on it. As a rule, I use an ICE for debugging program logic and most hardware problems. Critical timing problems in both hardware and software may call for other tools.

LOGIC ANALYZERS

Many programmers have never used logic analyzers, and may have been less effective as a result. They will tell you basically anything you want to know about the real-time behaviour of a system. The biggest problems with using them are doing the setup and filtering the data to get to the information you need.

A good example of this is a problem I ran into on a large Ada project. A critical load module would run fine under the ICE, but would die after about five minutes of running untethered. The error result was a coprocessor protocol violation between the 68020 and the 68881 processors. The address where it died was never the same. The question of the hour was a common one during system integration: was it software or hardware?

Obviously, ICE’s couldn’t be used to isolate the problem. I hooked up a Software Analysis Workstation, which is a logic analyzer sold by Cadre with a programmer’s user interface and examined what was going on.

I set the trace to break on the error and tell me what happened before it. It soon became apparent that the error only occurred on the coprocessor operation following a coprocessor operation that had been interrupted. A close look at the interrupt handling system code showed the assumption that all stack frames were created equal. The bits that signaled the 68020 to restore the coprocessor status registers from the stack frame were being overwritten, hosing the protocol from then on. Total time to find and fix the problem: one and a half days.

This is not to say that a logic analyzer is “better” than an ICE, only different. In general, an ICE is better at debugging logic problems, while a logic analyzer is more appropriate for problems related to system timing. The moral is that the correct tool used intelligently is the shortest path between a problem and the solution.

HYBRID DEVICES

A relatively recent addition to the tools that are available are ICE’s that have logic analyzers built into the front end. This potent combination provides the sophisticated triggering capabilities of a logic analyzer in conjunction with the control of an ICE. Most of the high-end vendors of ICE’s have taken this approach, and for good reason. It allows them to keep providing systems to support ever more sophisticated target processors.

On the other side of the fence, some logic analyzers are beginning to gain control functions formerly reserved for ICE’s. An example of this is the Tektronix Prism series, with the optional Programmer’s Debug Tool (PDT) ROM emulator. This setup provides a plug into ROM sockets on the target system, which it uses to provide instructions and data to the microprocessor. When a break in CPU flow is called for, a break instruction can be inserted into the program flow or an interrupt line can be activated, whichever is appropriate for the particular processor being used. In general, these devices provide a useful subset of the functionality of a full ICE at a lower price.

This also applies to devices such as the CodeTap, or the various ROM emulators that are available. These devices may be all that’s needed in many situations, and may be used instead of or to supplement a facility’s supply of ICES. Check carefully into exactly what functions they do provide, to make sure they will meet your needs.

ORGANIZATIONAL CONSIDERATIONS

Debugging is largely a human activity, so any discussion which only covers the technical aspects is incomplete. I have formulated a couple of general rules that have so far stood the test of time. The first of these is:

1. Debug a system as a system.

The industrial revolution taught us that work could be divided, allowing larger systems to be built. Unfortunately, that division is usually made along "functional" lines, leading to separate groups developing hardware and software, often subdivided further into those having responsibility for pieces of the hardware and software. This leads inevitably to finger...
It took several days, but the call did come. The system was getting an illegal instruction trap at a particular address. I used the ICE to examine that address, seeing what was indeed an illegal instruction. The corresponding byte in the load module differed by a single bit. Changing the value to the correct one allowed the code to run correctly.

I took advantage of the extra memory provided by the ICE to load the code twice, once at the correct location and once at a higher base address. I then had the ICE compare the two areas. The bit had been set wrong only in the lower memory area. It turned out that there was a memory error that caused that bit to be overwritten when a location 4096 bytes away was set. If the two happened to be the same, no problem. If they differed, flakiness resulted. I used the ICE to remap that area into ICE memory instead of target, and all problems went away.

The key to full use of an ICE is to understand fully the degree of control it really does provide. ICE memory can be used to supplement a stingy target, allowing the addition of test routines to the code to assist debugging. Watchpoints can be set to determine what part of the code is overwriting sensitive memory areas. It is also a great tool for ad hoc testing of hardware, since values can be poked into registers and the values read back without the need for writing code.

The other necessity for effective ICE use is to understand what it will not do. Vendor claims can lead you to assume that system behaviour under ICE control is exactly as it is when the ICE isn’t installed. I tend to treat this as a pleasant surprise when it occurs, but I generally don’t count on it. As a rule, I use an ICE for debugging program logic and most hardware

LOGIC ANALYZERS

Many programmers have never used logic analyzers, and may have been less effective as a result. They will tell you basically anything you want to know about the realtime behaviour of a system. The biggest problems with using them are doing the setup and filtering the data to get to the information you need.

A good example of this is a problem I ran into on a large Ada project. A critical load module would run fine under the ICE, but would die after about five minutes of running untethered. The error result was a coprocessor protocol violation between the 68020 and the 68881 processors. The address where it died was never the same. The question of the hour was a common one during system integration: was it software or hardware?

Obviously, ICE’s couldn’t be used to isolate the problem. I hooked up a Software Analysis Workstation, which is a logic analyzer sold by Cadre with a programmer’s user interface and examined what was going on.

I set the trace to break on the error and tell me what happened before it. It soon became apparent that the error only occurred on the coprocessor operation following a coprocessor operation that had been interrupted. A close look at the interrupt handling system code showed the assumption that all stack frames were created equal. The bits that signaled the 68020 to restore the coprocessor status registers from the stack frame were being overwritten, hosing the protocol from then on. Total time to find and fix the problem: one and a half days.

This is not to say that a logic analyzer is “better” than an ICE, only different. In general, an ICE is better at debugging logic problems, while a logic analyzer is more appropriate for problems related to system timing. The moral is that the correct tool used intelligently is the shortest path between a problem and the solution.

HYBRID DEVICES

A relatively recent addition to the tools that are available are ICE’s that have logic analyzers built into the front end. This potent combination provides the sophisticated triggering capabilities of a logic analyzer in conjunction with the control of an ICE. Most of the high-end vendors of ICE’s have taken this approach, and for good reason. It allows them to keep providing systems to support ever more sophisticated target processors.

On the other side of the fence, some logic analyzers are beginning to gain control functions formerly reserved for ICE’s. An example of this is the Tektronix Prism series, with the optional Programmer’s Debug Tool (PDT) ROM emulator. This setup provides a plug into ROM sockets on the target system, which it uses to provide instructions and data to the microprocessor. When a break in CPU flow is called for, a break instruction can be inserted into the program flow or an interrupt line can be activated, whichever is appropriate for the particular processor being used. In general, these devices provide a useful subset of the functionality of a full ICE at a lower price.

This also applies to devices such as the CodeTap, or the various ROM emulators that are available. These devices may be all that’s needed in many situations, and may be used instead of or to supplement a facility’s supply of ICES. Check carefully into exactly what functions they do provide, to make sure they will meet your needs.

ORGANIZATIONAL CONSIDERATIONS

Debugging is largely a human activity, so any discussion which only covers the technical aspects is incomplete. I have formulated a couple of general rules that have so far stood the test of time. The first of these is:

1. Debug a system as a system.

The industrial revolution taught us that work could be divided, allowing larger systems to be built. Unfortunately, that division is usually made along "functional" lines, leading to separate groups developing hardware and software, often subdivided further into those having responsibility for pieces of the hardware and software. This leads inevitably to finger
pointing during system integration, since it is in the best interests of each group to have problems found in the others.

I ran into this problem in a large project. The hardware was horribly late, a fact used by the software group to slip schedules obscenely. When the hardware finally started arriving, it came to light that software was in at least as bad shape. There was no sympathy or support from the hardware group, since they still wore the scars inflicted by software management.

I was called in to work with a group of hardware engineers on a subsystem redesign on this project. I had been working with them for a while, and there was a large degree of mutual respect. I realized how different the atmosphere was when I was discussing the 68020/68881 problem described above with the lead hardware engineer whose group had selected the board. He was convinced it was a hardware problem, while I maintained it was software. I “won” the argument by proving the problem was in code written by my group. He took defeat gracefully.

2. Use tools before you need them.

I have often seen test and debug equipment sitting unused in a corner of the lab while engineers work feverishly to put out fires. The common explanation is that they don’t have time to learn to use new equipment when they are working on the latest drop-deadline. Earlier in the project, when they were working on easier problems, they didn’t need the help the new equipment would have given them, so the time wasn’t allocated then, either.

People under pressure will revert to techniques that have worked for them in the past. The time to introduce new tools is before they are needed, and people should be encouraged strongly to use them, even if the old tools are still working for them. This will give them a wider repertoire to call on when crunch time hits, as it inevitably does.

CONCLUSION

Embedded systems programming is by nature a multidisciplinary activity. The wider scope of knowledge necessary to perform this activity effectively can be a burden, but the reward is in having a range of types of tools available. A programmer that doesn’t take full advantage of these tools is tilting at bigger windmills without the benefit of bigger, better lances.