



## Developing WDM Device Drivers For Windows

This is an intensive program intended at explaining the core concepts involved in Windows Driver development using the Windows Driver Model (WDM) framework. It is intended for device driver and device firmware writers for writing function/client drivers for devices such as audio, parallel/serial port and other devices.

Pre-requisites:

- A. Sound knowledge of C programming (Must)
- B. Knowledge of Windows OS Internals (Must)
- C. Basic H/W device concepts such as memory mapping, port access, device registers etc. (Must)
- D. Communication protocols (Desirable)

The key learning from the program are:

- A. Structure of WDM drivers
- B. I/O Request data structures, handling and management
- C. Introduction to Plug'n'Play and Power Management concepts
- D. Device IO Control mechanisms
- E. Debugging drivers

### Day 1 Basic Structure of a WDM Driver

- How Drivers Work
- How Applications Work
- Device Drivers How the System Finds and Loads Drivers
- Device and Driver Layering
- Plug and Play Devices
- Legacy Devices
- IRP Routing
- The Two Basic Data Structures
  - Driver objects
  - Device objects
- Overview of *DriverEntry*, *DriverUnload* and *AddDevice* Routines
- Creating a Device object
- Naming Devices

### Day 2 The I/O Request Packet Data Structures

- Structure of an IRP
- The I/O Stack The "Standard Model" for IRP Processing
- Creating an IRP
- Forwarding to a Dispatch Routine
- Duties of a Dispatch Routine
- The *StartIo* Routine
- The Interrupt Service Routine

- Deferred Procedure Call Routine
- I/O Completion Routines
- Queuing I/O Requests
- The *DEVQUEUE* object
- Cancelling I/O Requests
- Completing the Dispatch Routine
- Asynchronous IRPs
- Synchronous IRPs

### **Day 3 Plug and Play for Function Drivers**

- *IRP\_MJ\_PNP* Dispatch Function
- Starting and Stopping Your Device
  - *IRP\_MN\_START\_DEVICE*
  - *IRP\_MN\_STOP\_DEVICE*
  - *IRP\_MN\_REMOVE\_DEVICE*
  - *IRP\_MN\_SURPRISE\_REMOVAL*
- Managing PnP State Transitions
  - Starting the Device
  - While the Device Is Stopped
  - Synchronizing Removal

### **Reading and Writing Data**

- Configuring Your Device
- Addressing a Data Buffer
  - Specifying a Buffering Method
- Ports and Registers
  - Port Resources
  - Memory Resources
- Servicing an Interrupt
  - Configuring an Interrupt
  - Handling Interrupts
  - Deferred Procedure Calls
  - A Simple Interrupt-Driven Device
- Direct Memory Access
  - Transfer Strategies
  - Performing DMA Transfers
  - Using a Common Buffer

### **Day 4 Power Management and I/O Control**

#### **Power Management**

- The WDM Power Model
  - The Roles of WDM Drivers
  - Device Power and System Power States
  - Power State Transitions

- Handling *IRP\_MJ\_POWER* Requests
- Managing Power Transitions
  - Required Infrastructure
  - System Power IRPs That Increase Power
  - System Power IRPs That Decrease Power
  - Device Power IRPs

### **I/O Control Operations**

- The *DeviceIoControl* API
  - Synchronous and Asynchronous Calls to *DeviceIoControl*
  - Defining I/O Control Codes
- Handling *IRP\_MJ\_DEVICE\_CONTROL*
  - *METHOD\_BUFFERED*
  - The *DIRECT* Buffering Methods
  - *METHOD\_NEITHER*
  - Designing a Safe and Secure IOCTL Interface
- Internal I/O Control operations
- Notifying Applications of Events
  - Using a Shared Event for Notification
  - Using a Pending IOCTL for Notification

### **Day 5 Distributing and Testing Device Drivers**

- **The Role of the Registry**
  - The Hardware (Instance) Key
  - The Class Key
  - The Driver Key
  - The Service (Software) Key
  - Accessing the Registry from a Program
  - Device Object Properties
- **The INF File**
  - Install Sections
  - Populating the Registry
  - Security Settings
  - Device Identifiers
  - Driver Ranking
  - Tools for INF Files

### **Testing and Debugging Drivers**

- Reading CRASH Screens
  - Layout of a STOP Message
  - Deciphering STOP Messages



- Overview of WinDbg
- Analyzing a Crash Dump
  - Goals of the Analysis
  - Starting the Analysis
  - Tracing the Stack

\* \* \* \* \*