WinFT ODK v2.1, 3.0 and 4.0 for Windows 95, NT and CE

High-Reliability Win32 Embedded Systems

Product Overview

WinFT™ delivers fault detection and correction features for new and legacy Win32 applications, including Windows CE. It provides fault tolerance at the application level, enabling the discovery of and recovery from faults that cannot be resolved by hardware techniques or by the operating system.

The requirement for high-reliability Win32-based embedded applications is ever increasing. While there are high-reliability, fault-tolerant hardware and operating systems solutions on the market, high-reliability features also need to be incorporated in the applications themselves. This effort has traditionally been left to the developer who must design and hard code these features directly within the applications.

WinFT provides a ready-made API and software Watchdog Server framework that eliminates the need to develop custom code for typical high-reliability features such exception handling, check-pointing or restarting. Using the simple WinFT API, developers can quickly and easily build in fault-tolerant features into their applications. In addition, the WinFT Watchdog Server can monitor and restart legacy Win32 applications and processes without programming.

WinFT was originally developed to provide fault tolerance in industrial control Win32 applications where reliability requirements dictate high service availability. Other industries where applications can benefit from WinFT's fault tolerant capabilities include: online transaction processing, telecommunications, and retail. For Windows CE systems, WinFT can be used in conjunction with the Rainbow web server to provide full control of remote applications.

WinFT can help Win32 application developers and users in these and other markets easily increase the reliability and availability of their systems.

Features and Benefits

Simple to administer - a simple Watchdog Server to configure which applications and services are monitored and how faults and events are dealt with;

Support for legacy applications – the ability to monitor and restart existing Win32 applications and processes with no programming required.

Powerful Application Programming Interface - the ODK includes an API that gives developers the ability to incorporate high reliability features right into their new application. This then yields a powerful and tight coupling between the Watchdog Server and the WinFT-enabled applications.

Critical data persistence - application data can be preserved to disk during critical points of operation. If the application fails during checkpoints, the application is restarted using the saved data from the previous checkpoint.

Fault and event logging - system wide and application fault logging capabilities.

Rejuvenation - system refreshing through controlled application or operating system shutdowns and restarts.

Broad platform support – DeviceCOM can operate on Windows NT 4.0, Windows 95, and Windows CE platforms.

Complements other fault tolerant architectures - WinFT can further enhance the service reliability of applications running over existing fault tolerant hardware and/or operating systems.

Cost effectiveness - Since WinFT is a software solution, it offers the option to add fault tolerance to applications where traditional fault tolerant architectures would either be too complex or costly to include. This is particularly true in embedded applications.

INTRINSYC Software Inc.

Technology Overview

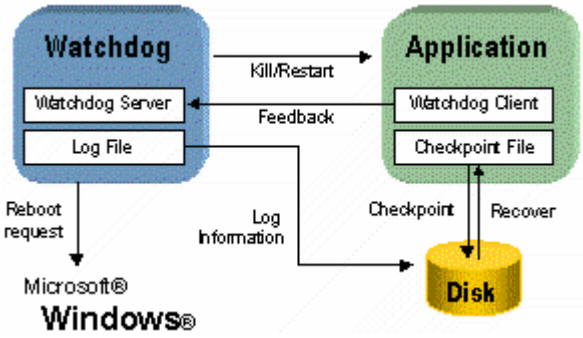
For WinFT-instrumented applications or services, the Watchdog Server can detect and restarts crashed or hung processes. Instrumented applications monitored by the Watchdog Server periodically transmit an "alive" message to the Server. If the Watchdog Server does not receive an "alive" message in a timeout specified in the Watchdog Server configuration, the application process will be terminated (if it still exists) and a new process created.

Non-instrumented legacy applications monitored by the Watchdog Server will be restarted if the process has terminated for any reason or if it has performed an illegal operation (e.g. it has generated an unhandled exception).

If the restart of an application fails several times, perhaps due to some operating system or correctable hardware failure, the system can be automatically rebooted and the application restarted. The precise conditions under which the system is rebooted can be specified in the Watchdog Server.

Instrumented applications monitored by the Watchdog Server can also transmit "error" messages to the Watchdog Server. For example, an application may transmit the message "Failed to open database. Remote host is unavailable." If the Watchdog Server receives a number of errors exceeding a certain tolerance (as specified by the administrator on an application by application basis) the application may be restarted or the system may be rebooted (also as specified by the administrator). Non-instrumented legacy applications do not transmit error messages.

Software rejuvenation is a preventative measure. It consists of gracefully terminating a persistent application at an opportune time (i.e. it is not busy) and restarting it, or rebooting the operating system at an opportune time. Instrumented applications monitored by the Watchdog Server can transmit "idle" messages to the Server. If a configurable number of idle messages are received in a specified interval, the application is restarted. Non-instrumented legacy applications do not transmit "idle" messages, and consequently do not support



software rejuvenation. The handling of "I'm alive", "error" and "idle" messages is entirely at the control of the administrator on an application by application basis by interacting with the Watchdog Server.

Check-pointing consists of saving essential application data to disk during critical points of operation. If the application fails between checkpoints, the application is restarted using the saved data from the last checkpoint.

The WinFT log provides information on the overall performance of the system as well as historical data about executables and exceptions.

Contact Information

Intrinsyc Software, Inc.
Suite 1050, 1075 W. Georgia St.
Vancouver, BC, V6E 3C9
Tel: (604) 801-6461
Fax: (619) 673-1432
E-mail: sales@intrinsyc.com
Web: www.intrinsyc.com

Specifications

V2.1 System Requirements:
- Microsoft Windows 95 & NT 4.0
- Microsoft Visual C++ v5.0

V3.0 System Requirements
- Microsoft Windows NT 4.0 only
- Microsoft Visual C++ v5.0

V4.0 System Requirements (preliminary)
- Microsoft Windows CE 2.0, NT 4.0
- Microsoft Windows CE Toolkit for VC++ 5.0

V2.1 Capabilities
- Watchdog Server runs as an application only
- Monitors applications only

V3.0 Capabilities
- Watchdog Server runs as a service only
- Monitors applications and services

V4.0 Capabilities (preliminary)
- Contact Intrinsyc for details